Novell®
Sentinel™

5.1.3

www.novell.com

Volume I – GUIA DE INSTALAÇÃO

7 de julho, 2006

Novell®

Informações legais

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
EUA
www.novell.com

Documentação Online: Para acessar a documentação online deste produto e de outros produtos da Novell e obter atualizações,visite www.novell.com/documentation.

Marcas registradas da Novell

Para obter informações sobre as marcas registradas da Novell, consulte a lista Marcas registradas da Novell e marcas de serviços em (http://www.novell.com/company/legal/trademarks/tmlist.html).

Materiais de terceiros

Todas as marcas registradas de terceiros pertencem aos seus respectivos proprietários.

Informações legais de terceiros

O Sentinel 5 pode conter as seguintes tecnologias de terceiros:

- Apache Axis e Apache Tomcat, Copyright © 1999 a 2005, Apache Software Foundation. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://www.apache.org/licenses/
- ANTLR. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://www.antlr.org
- Boost, Copyright © 1999, Boost.org.
- Bouncy Castle, Copyright © 2000-2004, the Legion of Bouncy Castle. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://www.bouncycastle.org.
- Checkpoint. Copyright © Check Point Software Technologies Ltd.
- Concurrent, pacote de utilitários. Copyright © Doug Lea. Usado sem as classes CopyOnWriteArrayList e ConcurrentReaderHashMap.
- Crypto++ Compilation. Copyright © 1995-2003, Wei Dai, incorporando o seguinte trabalho protegido por lei de direitos autorais: mars.cpp por Brian Gladman e Sean Woods. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://www.eskimo.com/~weidai/License.txt.
- Crystal Reports Developer e Crystal Reports Server. Copyright © 2004 Business Objects Software Limited.
- DataDirect Technologies Corp. Copyright © 1991-2003.
- edpFTPj, licenciado sob a Licença Pública GNU Menos Restritiva. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://www.enterprisedt.com/products/edtftpj/purchase.html.
- Enhydra Shark, licenciado sob a Licença Pública GNU Menos Restritiva, disponível em: http://shark.objectweb.org/license.html.
- ICEsoft ICEbrowser. ICEsoft Technologies, Inc. Copyright © 2003-2004.
- ILOG, Inc. Copyright © 1999-2004.
- Installshield Universal. Copyright © 1996–2005, Macrovision Corporation e/ou Macrovision Europe Ltd.
- Java 2 Platform, Standard Edition. Copyright © Sun Microsystems, Inc. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://java.sun.com/j2se/1.4.2/j2re-1_4_2_10-license.txt.

  O Java 2 Platform também pode conter os seguintes produtos de terceiros:

  - CoolServlets © 1999
  - DES e 3xDES © 2000 por Jef Poskanzer
  - Crimson © 1999-2000 The Apache Software Foundation
  - Xalan J2 © 1999-2000 The Apache Software Foundation
  - NSIS 1.0j © 1999-2000 Nullsoft, Inc.
  - Eastman Kodak Company © 1992

- Lucinda, uma marca comercial registrada ou marca registrada da Bigelow e Holmes
- Taligent, Inc.
- IBM, algumas partes disponíveis em: http://oss.software.ibm.com/icu4j/

Para obter mais informações sobre essas tecnologias de terceiros e suas isenções de responsabilidade e restrições associadas, consulte: http://java.sun.com/j2se/1.4.2/j2se-1_4_2-thirdpartylicensereadme.txt.

- JavaBeans Activation Framework (JAF). Copyright © Sun Microsystems, Inc. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://www.java.sun.com/products/javabeans/glasgow/jaf.html e clique em download > license.
- JavaMail. Copyright © Sun Microsystems, Inc. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://www.java.sun.com/products/javamail/downloads/index.html e clique em download > license.
- Java Ace, por Douglas C. Schmidt e seu grupo de pesquisa na Washington University e Tao (with ACE wrappers) por Douglas C. Schmidt e seu grupo de pesquisa em Washington University, University of California, Irvine e Vanderbilt University. Copyright © 1993-2005.Para obter mais informações, isenções de responsabilidade e restrições, consulte http://www.cs.wustl.edu/~schmidt/ACE-copying.html e http://www.cs.wustl.edu/~pjain/java/ace/JACE-copying.html
- Java Authentication e Authorization Service Modules, licenciados sob a Licença Pública Geral Menos Restritiva. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://free.tagish.net/jaas/index.jsp.
- Java Network Launching Protocol (JNLP). Copyright © Sun Microsystems, Inc. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://www.java.sun.com/products/javawebstart/downloads-jnlp.html e clique em download > license.
- Java Service Wrapper. Partes protegidas por lei de direitos autorais da seguinte maneira: Copyright © 1999, 2004 Tanuki Software e Copyright © 2001 Silver Egg Technology. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://wrapper.tanukisoftware.org/doc/english/license.html.
- JIDE. Copyright © 2002 a 2005, JIDE Software, Inc.
- O jTDS é licenciado sob a Licença Pública GNU Menos Restritiva. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://jtds.sourceforge.net/.
- MDateSelector. Copyright © 2005, Martin Newstead, licenciado sobre a Licença Pública Geral Menos Restritiva. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://web.ukonline.co.uk/mseries.
- Monarch Charts. Copyright © 2005, Singleton Labs.
- Net-SNMP. Partes do código são protegidas por lei de direitos autorais por várias entidades, que se reservam todos os direitos. Copyright © 1989, 1991, 1992 por Carnegie Mellon University; Copyright © 1996, 1998 a 2000, the Regents of the University of California; Copyright © 2001 a 2003 Networks Associates Technology, Inc.; Copyright © 2001 a 2003, Cambridge Broadband, Ltd.; Copyright © 2003 Sun Microsystems, Inc. e Copyright © 2003 a 2004, Sparta, Inc. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://net-snmp.sourceforge.net.
- The OpenSSL Project. Copyright © 1998-2004. the Open SSL Project. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://www.openssl.org.
- Oracle Help for Java. Copyright © 1994-2006, Oracle Corporation.
- RoboHELP Office. Copyright © Adobe Systems Incorporated, antiga Macromedia.
- Skin Look and Feel (SkinLF). Copyright © 2000-2006 L2FProd.com. Licenciado sob a Licença de Software do Apache. Para obter mais informações, isenções de responsabilidade e restrições, consulte https://skinlf.dev.java.net/.
- Sonic Software Corporation. Copyright © 2003-2004. O software SSC contém software de segurança licenciado pela RSA Security, Inc.

Prefácio

A documentação técnica do Sentinel consiste no guia de referência e operação para finalidade geral. Essa documentação é destinada aos profissionais de segurança da informação. O texto foi desenvolvido para ser usado como fonte de referência sobre o Sistema de Gerenciamento de Segurança Empresarial do Sentinel. A documentação adicional está disponível no portal do Sentinel na Web.

A documentação técnica do Sentinel está dividida em cinco volumes. São eles:

- Volume I – Guia de Instalação do Sentinel™ 5
- Volume II – Guia do Usuário do Sentinel™ 5
- Volume III – Guia do Usuário do Assistente do Sentinel™ 5
- Volume IV – Guia de Referência do Usuário do Sentinel™ 5
- Volume V – Integração de Terceiros do Sentinel™ 5

Volume I – Guia de Instalação do Sentinel

Este guia explica como instalar:

- Sentinel Server
- Console do Sentinel
- Mecanismo de Correlação do Sentinel
- Crystal Reports do Sentinel
- Construtor de Coletor Assistente
- Gerenciador de Coletor Assistente
- Advisor

Volume II – Guia do Usuário do Sentinel

Este guia aborda o seguinte:

- Operação do Console do Sentinel
- Recursos do Sentinel
- Arquitetura do Sentinel
- Comunicação do Sentinel
- Encerramento/Inicialização do Sentinel
- Avaliação de vulnerabilidade
- Monitoramento de eventos
- Filtragem de eventos
- Correlação de eventos
- Gerenciador de Dados do Sentinel
- Configuração de Eventos para Relevância Comercial
- Serviço de Mapeamento
- Geração de relatórios de histórico
- Gerenciamento de Host do Assistente
- Incidentes
- Casos
- Gerenciamento de usuários
- Workflow

Volume III – Guia do Usuário do Assistente

Este guia aborda o seguinte:

- Operação do Construtor de Coletor Assistente
- Gerenciador de Coletor Assistente
- Coletores
- Gerenciamento de Host do Assistente
- Construção e manutenção de coletores

Volue IV – Guia de Referência do Usuário do Sentinel

Este guia aborda o seguinte:

- Linguagem de criação de scripts do assistente
- Comandos de análise do Assistente
- Funções do administrador do Assistente
- Metatags do Assistente e do Sentinel
- Permissões de usuário
- Mecanismo de correlação do Sentinel
- Opções da linha de comando de correlação
- Esquema do banco de dados do Sentinel

Volume V – Guia de Integração de Terceiros do Sentinel

- Remedy
- Operações do HP OpenView
- HP Service Desk

Sumário

8 Patch para Oracle no Linux 8-1

9 Crystal Reports para Windows e Solaris 9-1

10 Crystal Reports para Linux 10-1

1 Introdução

NOTA: O termo Agente é sinônimo de Coletor. De agora em diante, Agentes serão referidos como Coletores.

Esse guia orientará uma instalação básica. O Guia do Usuário do Sentinel™ 5 apresenta mais detalhes da arquitetura, operação e procedimentos administrativos.

Este guia supõe que você está familiarizado com segurança de rede, administração de bancos de dados e dos sistemas operacionais Windows e UNIX.

Convenções usadas

Nota e avisos

NOTA: As notas apresentam informações adicionais que podem ser úteis.

AVISO: Os avisos apresentam informações adicionais que podem impedir danos ou perda de dados do sistema.

Comandos

Os comandos aparecem na fonte Courier. Por exemplo:

```
useradd –g dba –d /export/home/oracle –m –s /bin/csh
   oracle
```

Visão geral do Sentinel 5

O Sentinel 5 garante o que você deve exigir de uma solução de gerenciamento de informações de segurança. O Sentinel 5 inclui capacidades de gerenciamento de informações de segurança padrão, tais como coletar, reunir, correlacionar e exibir dados de eventos. Ele também permite que você responda de modo apropriado e decisivo aos incidentes, automatizando e garantindo sua identificação e os processos de resolução.

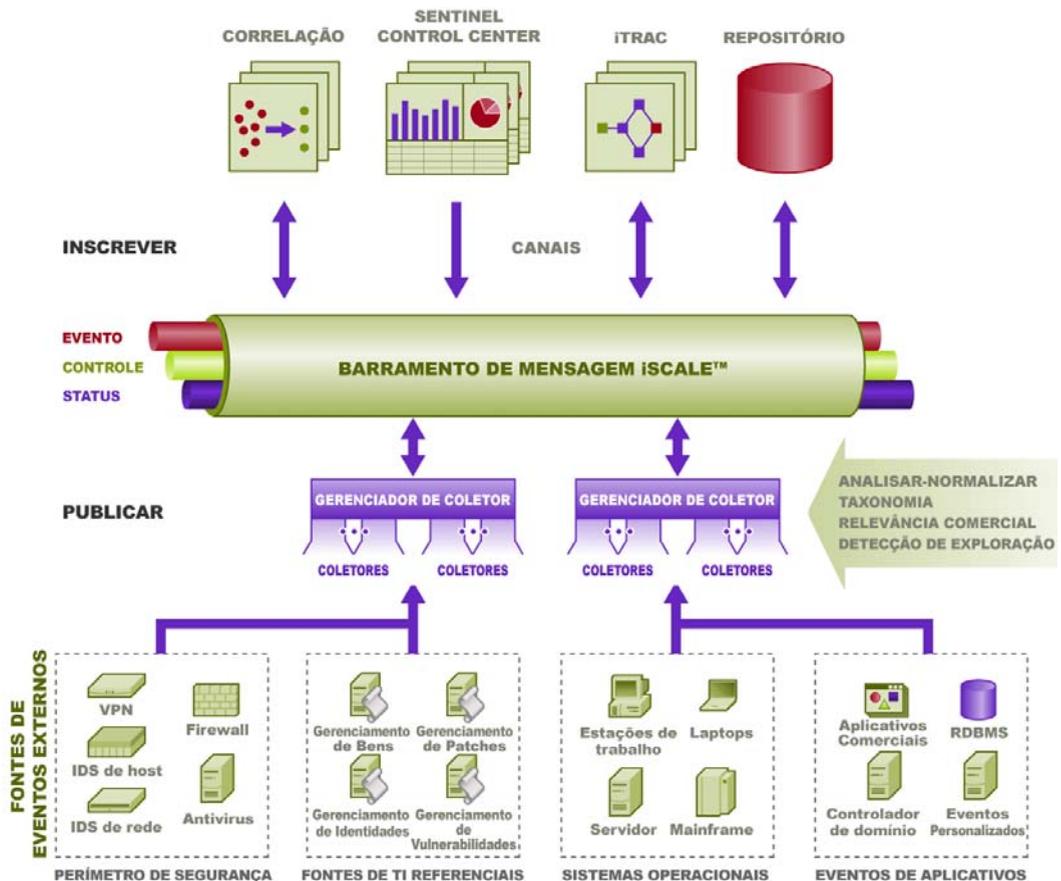
Os recursos principais do Sentinel 5 são iTRAC™, Active Views™ e iSCALE™. Isso permite gerenciar, medir e administrar de modo mais eficiente. Com o Sentinel 5, você pode:

- Obter visibilidade e o controle necessário para gerenciar seu ambiente de segurança com uma melhor relação custo-benefício
- Detectar e resolver incidentes mais rapidamente, enquanto reduz os custos operacionais
- Fornecer relatórios adequados e métricas para avaliar continuamente a segurança e a postura de conformidade
- Alcançar e monitorar a conformidade com as normas e políticas governamentais.

Realizar mais tarefas com os recursos atuais eliminando os processos manuais

O Sentinel 5 é composto de vários componentes que atuam em conjunto para formar a solução líder do mercado:

- Sentinel Control Center
- Sentinel Server
- Sentinel Advisor
- Gerenciador de Dados do Sentinel
- Sentinel Wizard
  - Construtor de Coletor Assistente
  - Gerenciador de Coletor Assistente
  - Mecanismo de Assistente

A seguir, uma **arquitetura conceitual** do Sentinel 5, que ilustra os componentes do Sentinel envolvidos na realização do Gerenciamento de Segurança.

Módulos do produto do Sentinel

O Sentinel 5 é composto de três módulos primários – Sentinel Control Center, Sentinel Wizard (Construtor de Coletor e Gerenciador de Coletor) e Sentinel Advisor.

Sentinel Control Center

O Sentinel Control Center oferece um painel de gerenciamento de segurança integrado que permite que os analistas identifiquem rapidamente as novas tendências ou ataques, manipulem e interajam com informações gráficas em tempo real e respondam a incidentes. Os recursos principais do Sentinel Control Center incluem:

- Active Views – análises e visualizações em tempo real
- Incidentes – criação e gerenciamento de incidentes
- Admin – definição e gerenciamento de regras de correlação
- iTRACc – gerenciamento de processos de documentação, aplicação e rastreamento dos processos de resolução de incidentes.
- Relatórios – métricas e relatórios de histórico

Sentinel Wizard

O Sentinel Wizard coleta dados de dispositivos fonte e fornece um fluxo de eventos enriquecido injetando taxonomia, detecção de exploração e relevância de negócios no fluxo de dados antes dos eventos serem correlacionados, analisados e enviados para o banco de dados. Um fluxo de eventos enriquecido significa que os dados estão correlacionados ao contexto comercial necessário para identificar e resolver ameaças internas ou externas e violações às políticas. Em qualquer configuração, pode haver um ou mais Assistentes distribuídos, proporcionando aos clientes a capacidade de distribuir componentes do produto na infra-estrutura da empresa, de acordo com sua topologia de rede.

O Wizard permite desenvolver e personalizar com eficiência os Coletores. Isso permite que o Sentinel colete dados de vários dispositivos diferentes em uma empresa. Esses dispositivos consistem de (mas não apenas):

- Sistemas de detecção de intrusão (host)
- Sistemas de detecção de intrusão (rede)
- Firewalls
- Sistemas operacionais
- Monitoramento de políticas
- Autenticação
- Roteadores e Switches
- VPN
- Antivírus
- Servidores da web
- Banco de dados
- Mainframe
- Avaliação de vulnerabilidade
- Serviços de diretório
- Gerenciador de Redes
- Sistemas proprietários

Os componentes principais do Sentinel Wizard incluem:

- Coletor – um receptor que coleta e normaliza eventos não processados (iniciais) de dispositivos e sistemas de segurança.
- Mecanismo do Coletor – componente que processa a lógica de gabarito para cada porta.
- O Gerenciador de Coletor – o componente final que gerencia os coletores, as mensagens de status do sistema e executa a filtragem global de eventos.
- O Construtor de Coletor – um aplicativo independente que permite construir e configurar coletores.

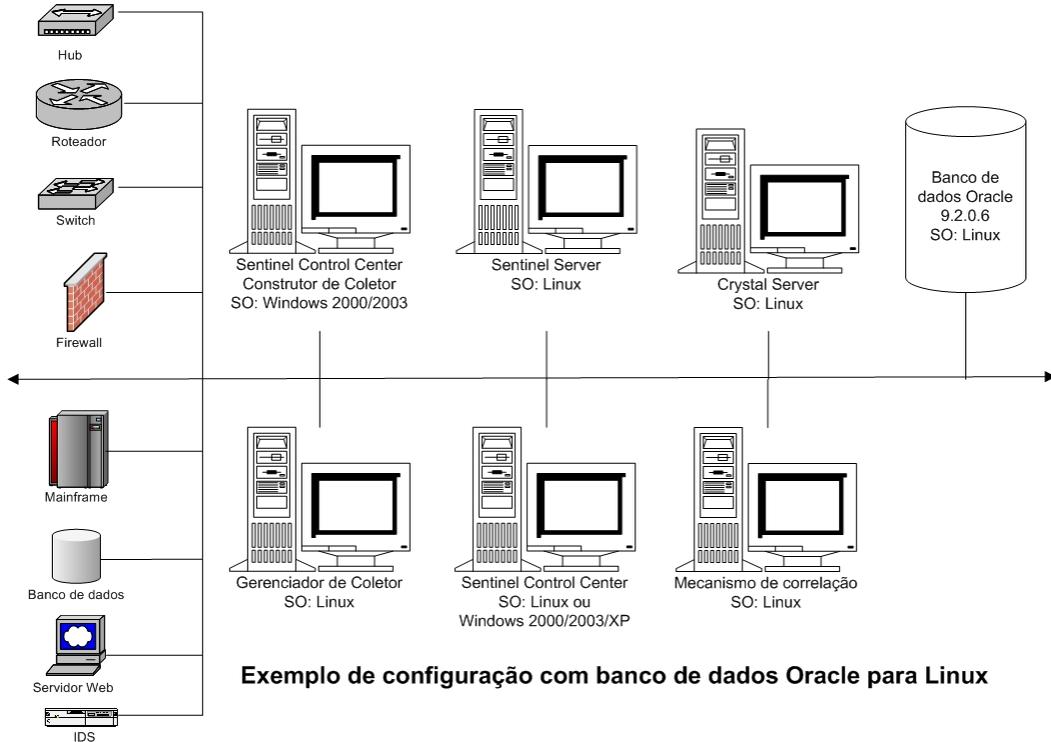
Sentinel Advisor

O Sentinel Advisor é um módulo opcional que efetua a referência cruzada entre os dados de alerta em tempo real do Sentinel com vulnerabilidades conhecidas e informações de resolução.

Configuração típica

A seguir, configurações típicas do Sentinel 5, que ilustram como o Gerenciamento de Segurança é feito. Sua implementação pode ser diferente dependendo de onde e como fez a instalação.

NOTA: Para obter informações específicas sobre o EPS (Eventos por segundo), Plataformas RAM, requisitos de espaço HDD e CPU, consulte o *Capítulo 2 - Melhores Práticas.*

Plataformas suportadas para o Sentinel Server no Linux

NOTA: Para sistemas operacionais específicos, consulte as tabelas a seguir.

Sentinel Server		
OS	**Versão**	**Nível de patch**
SuSE Linux Enterprise Server 9 (SLES 9)	9	
Red Hat Enterprise Linux	3	Atualização 5 ES (x86)

Banco de Dados		
Banco de Dados	**Versão**	**Nível de patch**
Oracle 64-bit Enterprise Edition	9i	▪ 9.2.0.6 2617419 ou ▪ 9.2.0.7

NOTA: Para obter mais informações sobre o Patch Crítico 2617419, consulte o site do Oracle e o Portal do Cliente Novell.

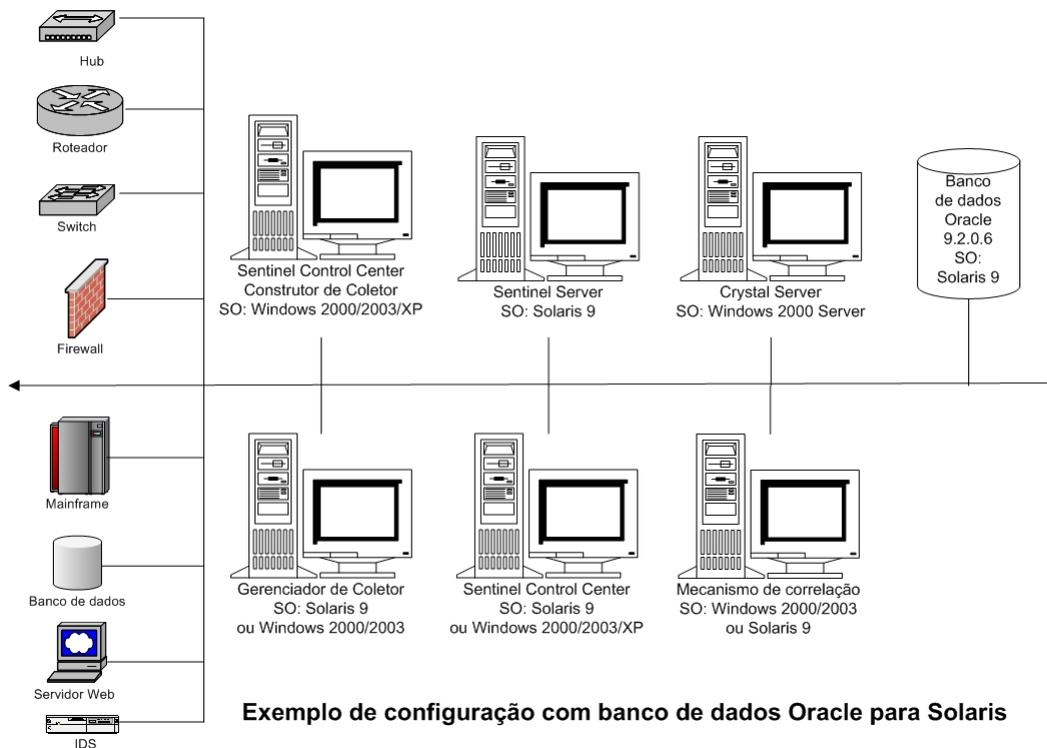
Sentinel Control Center (Interface de usuário)		
OS	**Versão**	**Nível de patch**
SuSE Linux Enterprise Server 9 (SLES 9)	9	
Red Hat Enterprise Linux	3	3 atualizações 5 ES (x86)
Windows	XP	SP1
Windows	2000	SP4
Windows	2003	SP1

Construtor de Coletor		
OS	**Versão**	**Nível de patch**
Windows	2000	SP4
Windows	2003	SP1

Gerenciador de Coletor		
OS	**Versão**	**Nível de patch**
Windows	2000	SP4
Windows	2003	SP1
Solaris	9	Patch Cluster recomendado do Solaris 9 DATA: 03/05/05
SuSE Linux Enterprise Server 9 (SLES 9)	9	
Red Hat Enterprise Linux	3	3 atualizações 5 ES (x86)

Crystal Server (Escolha de duas versões [Linux (SLES/Red Hat) e Windows])			
Versão do Crystal	**OS**	**Versão do OS**	**Nível de patch do OS**
Crystal BusinessObjects Enterprise™ 11	SuSE Linux Enterprise Server 9 (SLES 9)	9	
Crystal BusinessObjects Enterprise™ 11	Red Hat Enterprise Linux	3	3 atualizações 5 ES (x86)
Crystal BusinessObjects Enterprise™ 11	Windows com MS SQL 2000 Sentinel 5 não tem suporte para MSDE.	Windows 2003 Server.	SP1

NOTA: O Sentinel 5 não tem suporte para o Crystal XI no Windows® 2000 Server e MSDE.

Plataformas suportadas para o Sentinel Server no Solaris

Exemplo de configuração com banco de dados Oracle para Solaris

NOTA: Para sistemas operacionais específicos, consulte as tabelas a seguir.

Sentinel Server		
OS	**Versão**	**Nível de patch**
Solaris Enterprise Edition	9	Patch Cluster recomendado do Solaris 9 DATA: 03/05/05

Banco de Dados		
Banco de Dados	**Versão**	**Nível de patch**
Oracle 64-bit	9i	▪ 9.2.0.6 2617419 ou ▪ 9.2.0.7

NOTA: Para obter mais informações sobre o Patch Crítico 2617419, consulte o site do Oracle e o Portal do Cliente Novell.

Sentinel Control Center (Interface de usuário)		
OS	**Versão**	**Nível de patch**
Solaris	9	Patch Cluster recomendado do Solaris 9 DATA: 03/05/05
Windows	XP	SP1
Windows	2000	SP4
Windows	2003	SP1

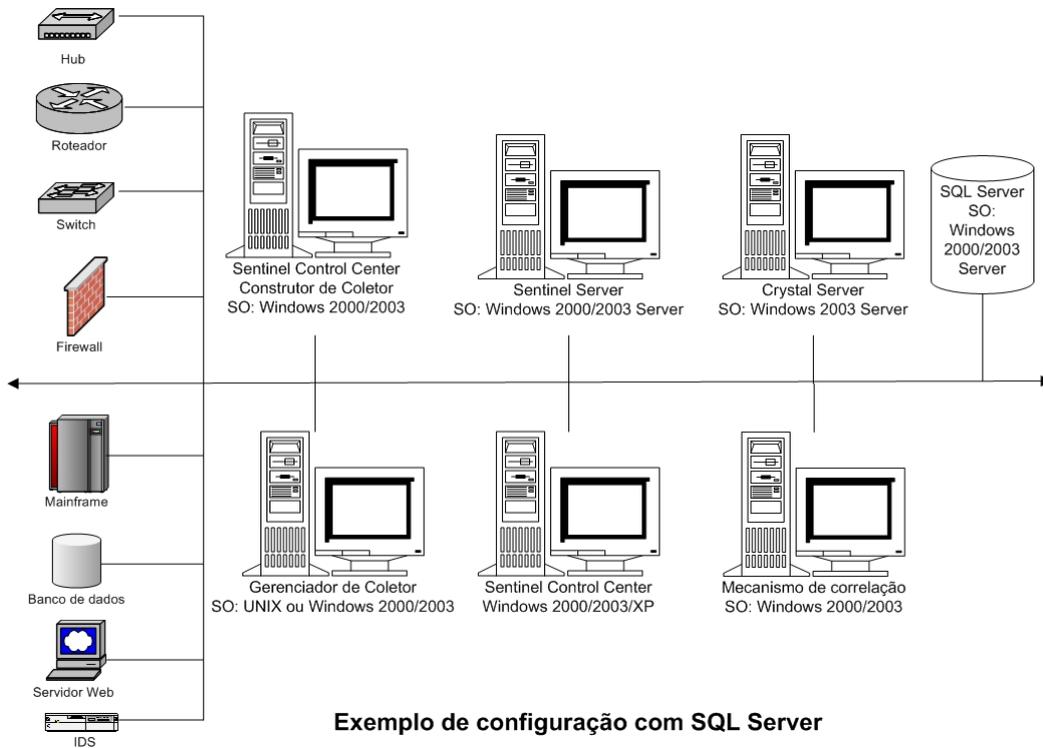
Construtor de Coletor		
OS	**Versão**	**Nível de patch**
Windows	2000	SP4
Windows	2003	SP1

Gerenciador de Coletor		
OS	**Versão**	**Nível de patch**
Windows	2000	SP4
Windows	2003	SP1
Solaris	9	Patch Cluster recomendado do Solaris 9 DATA: 03/05/05
SuSE Linux Enterprise Server 9 (SLES 9)	9	
Red Hat Enterprise Linux	3	3 atualizações 5 ES (x86)

Crystal Server			
Versão do Crystal	**OS**	**Versão do OS**	**Nível de patch do OS**
Crystal BusinessObjects Enterprise™ 11	Windows com MS SQL 2000 Sentinel 5 não tem suporte para MSDE.	Windows 2003 Server	SP1

NOTA: O Crystal Reports v9 é suportado no Sentinel v5.1 e anterior assim como o Sentinel v5.1.1 SP1 e posterior. Ele não é suportado no Sentinel v5.1.1 sem SP1. Se estiver usando o Crystal Reports v9 e Sentinel v5.1.1, você deve aplicar o Sentinel v5.1.1 Service Pack 1 ou atualizar para v5.1.2 ou v5.1.3.

NOTA: O Sentinel 5 não tem suporte para o Crystal XI no Windows® 2000 Server.

Plataformas suportadas para o Sentinel Server no Windows

Exemplo de configuração com SQL Server

NOTA: Para sistemas operacionais específicos, consulte as tabelas a seguir.

Sentinel Server		
OS	**Versão**	**Nível de patch**
Windows	2000 Server - Enterprise Edition	SP4
Windows	2003 Server - Enterprise Edition	SP1

Banco de Dados		
Banco de Dados	**Versão**	**Nível de patch**
SQL Server	2000 Enterprise	SP3a
SQL Server	2005 Enterprise (Sentinel v5.1.1 SP1 e posterior)	

Sentinel Control Center (Interface de usuário)		
OS	**Versão**	**Nível de patch**
Windows	XP	SP1
Windows	2000	SP4
Windows	2003	SP1

Construtor de Coletor		
OS	**Versão**	**Nível de patch**
Windows	2000	SP4
Windows	2003	SP1

Gerenciador de Coletor		
OS	**Versão**	**Nível de patch**
Windows	2000	SP4
Windows	2003	SP1
Solaris	9	Patch Cluster recomendado do Solaris 9 DATA: 03/05/05
SuSE Linux Enterprise Server 9 (SLES 9)	9	
Red Hat Enterprise Linux	3	3 atualizações 5 ES (x86)

Crystal Server			
Versão do Crystal	**OS**	**Versão do OS**	**Nível de patch do OS**
Crystal BusinessObjects Enterprise™ 11	Windows com MS SQL 2000 Sentinel 5 não tem suporte para MSDE.	Windows 2003 Server	SP1

NOTA: O Crystal Reports v9 é suportado no Sentinel v5.1 e anterior assim como o Sentinel v5.1.1 SP1 e posterior. Ele não é suportado no Sentinel v5.1.1 sem SP1. Se estiver usando o Crystal Reports v9 e Sentinel v5.1.1, você deve aplicar o Sentinel v5.1.1 Service Pack 1 ou atualizar para v5.1.2 ou v5.1.3.

NOTA: O Sentinel 5 não tem suporte para o Crystal XI no Windows® 2000 Server.

Outras referências da Novell

Os seguintes manuais estão disponíveis nos CDs de instalação do Sentinel.

- Guia de Instalação do Sentinel™
- Guia do Usuário do Sentinel™
- Guia do Usuário do Assistente do Sentinel™
- Guia de Referência do Usuário do Sentinel™
- Guia de Integração de terceiros do Sentinel™
- Notas da versão

Entrando em contato com a Novell

- Site na Web: www.novell.com
- Suporte Técnico da Novell: http://www.novell.com/support/index.html
- Suporte técnico internacional da Novell: http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup
- Auto atendimento: http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup
- Para obter suporte 24 horas por dia, 7 dias por semana, ligue 800-858-4000

2 Melhores práticas

NOTE: O termo Agente é sinônimo de Coletor. De agora em diante, Agentes serão referidos como Coletores.

Este capítulo aborda as melhores práticas e recomendações para o uso do Sentinel. Os tópicos incluem:

- Melhores práticas de instalação
  - Requisitos de hardware
  - Configuração de matriz de disco
  - Configuração de rede
  - Instalação de Oracle e MS SQL Server
  - Patches de banco de dados do e-SecuritySentinel
  - Configurações recomendadas de kernel UNIX
  - Parâmetros de configuração ao criar sua própria instância de banco de dados
  - Instalando o Sentinel
  - Maximizando a geração de relatórios de eventos para Crystal Reports
  - Relatórios fornecidos com o Sentinel
  - Dicas ao desenvolver relatórios Crystal personalizados
- Melhores práticas de manutenção
  - Análise de bancos de dados
  - Verificação da saúde do banco de dados
  - Arquivando dados e adicionando partições automaticamente (apenas Windows)
  - Mecanismo de correlação
  - Registro de transações
  - Locais de registro

Melhores práticas de instalação

A seguir estão as classificações de desempenho para atributos específicos do Sentinel.

Atributo	Classificação	Comentários
▪ EPS (Eventos por segundo) para inserção de BD de eventos	1250	A inserção é afetada por regras de correlação e pelo serviço de mapeamento.
▪ EPS para cada Gerenciador de Coletor	350	
▪ EPS por Coletor (Ponto de Verificação, Win2K etc...)	300	
▪ Número máximo de Coletores suportados por Gerenciador de Coletor	10	
▪ Máximo número de Gerenciadores de Coletor por Sentinel	20	
▪ Quantos regras são distribuídas por Mecanismo de correlação	20-80	Baixo EPS (150 EPS) = 80 Alto EPS (1250 EPS) = 20
▪ Quantas Telas Ativas™ por Sentinel	35 - 50	
▪ Número máximo de usuários simultâneos	20	
▪ Número máximo de telas por Sentinel Control Center	10	
▪ Número máximo de mapas por Sentinel	10	
▪ Tamanho máximo de cada Mapa	10 MB	
▪ Número máximo de linhas por mapa	350k	

A especificação de referência de CPU se baseia em:

- Windows - Xeon de 3,2 GHz
- SuSE Linux – Xeon de 3,2 GHz
- Solaris - Sparc-3 de 1,1 GHz
- Linux - Xeon de 3,2 GHz

A configuração é para os seguintes sistemas operacionais:

- Windows 2000 Server com SP4
- Windows 2003 Server com SP1
- SuSE Linux Enterprise Server 9 (SLES 9)
- Solaris 9 com patches com versão Generic_112233-11 do cluster de patch recomendado
- Atualização 5 ES do Red Hat Enterprise Linux 3 (x86)

O banco de dados é um dos seguintes:

- MSSQL 2000 com SP3a
- Oracle 9i Enterprise Edition 9.2.0.6 ou 9.2.0.7 com particionamento

Simples – Configuração Independente (utilização de demo)

Essa opção instala todos os componentes (inclusive o banco de dados) em uma única plataforma. Se destina principalmente a fins demonstrativos. Não é recomendada para uso real. Os requisitos de hardware são:

Componentes	**Mínimo**		**Recomendado**	
	RAM (GB)	**CPU**	**RAM (GB)**	**CPU**
Máquina 1 ▪ Todos os componentes do Sentinel ▪ Gerenciador de Coletor ▪ Coletores ▪ Banco de Dados ▪ Matriz de Disco Para Windows: ▪ Crystal Server ▪ Construtor de Coletor Para Linux: ▪ Crystal Server	2	2	4	2
Máquina 2 (apenas para instalações do UNIX) Para Solaris: ▪ Crystal Server ▪ Construtor de Coletor (Windows) Para Linux: ▪ Construtor de Coletor (Windows)	1.0	1	2.0	2

POC (Proof of Concept) – Configuração Independente

Essa opção instala todos os componentes, com exceção do banco de dados, em uma única plataforma. Essa configuração geralmente é usada para prova de conceitos, para testar a funcionalidade com cargas normais. Nesse caso, o banco de dados se encontra em uma máquina separada do restante do Sentinel.

Componentes	Mínimo		Recomendado	
	RAM (GB)	CPU	RAM (GB)	CPU
Máquina 1 ▪ Todos os componentes do Sentinel ▪ Gerenciador de Coletor ▪ Coletores Para Windows: ▪ Crystal Server ▪ Construtor de Coletor Para Linux: ▪ Crystal Server	4.0	2	4	4
Máquina 2 ▪ Banco de Dados ▪ Matriz de Disco	4	2	4	4
Máquina 3 (apenas para instalações do UNIX) Para Solaris: ▪ Crystal Server ▪ Construtor de Coletor (Windows) Para Linux: ▪ Construtor de Coletor (Windows)	2.0	2	4.0	2

Produção – Configuração distribuída

Uma Configuração distribuída é uma instalação personalizada que se destina a Sistemas Padrão e Empresariais.

Como o Sentinel tem oito componentes separados, além do Crystal Reports, há várias configurações diferentes que podem ser construídas. A seguir são abordadas duas configurações diferentes.

Como os bancos de dados dependem de E/S, é recomendável manter seu banco de dados em uma máquina separada. O servidor de BD exigirá uma matriz de armazenamento de alta velocidade que atenderá aos requisitos de E/S com base nas taxas de inserção de eventos.

Os hosts distribuídos devem ser conectados aos outros hosts Sentinel Server via um switch único de alta velocidade (GIGE) para impedir gargalos de tráfego de rede.

Produção – Configuração distribuída (Opção 1)

Configuração com quatro máquinas

Componentes	Mínimo		Recomendado	
	RAM (GB)	CPU	RAM (GB)	CPU
Máquina 1 ▪ Mecanismo de Correlação ▪ DAS ▪ iSCALE (Barramento de mensagens) ▪ Consultor	4.0	4	8.0	8
Máquina 2 ▪ Gerenciador de Coletor ▪ Coletores	1.0	2	2.0	2
Máquina 3 ▪ Crystal Server	2.0	2	4.0	4
Máquina 4 ▪ Banco de Dados ▪ Matriz de Disco	4	4	16	8

Produção – Configuração distribuída (Opção 2)

Configuração com cinco máquinas

Componentes	Mínimo		Recomendado	
	RAM (GB)	CPU	RAM (GB)	CPU
Máquina 1 ▪ DAS ▪ iSCALE (Barramento de mensagens) ▪ Consultor	4.0	4	8.0	8
Máquina 2 ▪ Mecanismo de Correlação	1.0	2	2.0	2
Máquina 3 ▪ Gerenciador de Coletor ▪ Coletores	1.0	2	2.0	2
Máquina 4 ▪ Crystal Server	2.0	2	4.0	4
Máquina 5 ▪ Banco de Dados ▪ Matriz de Disco	4	4	16	8

Política de suporte a patch

O Sentinel certificará os patches de sistemas operacionais e bancos de dados dentro de 60 dias a contar do lançamento.

Recomendações de hardware

Sentinel Server Mecanismo de Correlação			
EPS	**RAM**	**Espaço**	**CPU**
250	2 GB	72 GB	Windows - 24 x Xeon de 3,0 GHz SuSE Linux ou Redhat Linux - 24 x Xeon de 3,0 GHz Solaris - V280 2 x Ultra Sparc III de 1,1 GHz
500	4 GB	72 GB	Windows - 4 x Xeon de 3,0 GHz SuSE Linux ou Redhat Linux - 4 x Xeon de 3,0 GHz Solaris - V480 4 x Ultra Sparc III de 1,1 GHz
1000+	8 GB	72 GB	Windows - 8 x Xeon de 3,0 GHz SuSE Linux ou Redhat Linux - 84 x Xeon de 3,0 GHz Solaris - V880 8 x Ultra Sparc III de 1,1 GHz

Gerenciador de Coletor de Agente			
EPS	**RAM**	**Espaço**	**CPU**
250	2 GB	36 GB	Windows - 2 x Xeon de 3,0 GHz SuSE Linux ou Redhat Linux - 2 x Xeon de 3,0 GHz Solaris - V280 2 x Ultra Sparc III de 1,1 GHz
350+500	4 GB	36 GB	Windows - 4 x Xeon de 3,0 GHz SuSE Linux ou Redhat Linux - 4 x Xeon de 3,0 GHz Solaris - V480 4 x Ultra Sparc III de 1,1 GHz
1000+	8 GB	36 GB	Windows - 8 x Xeon de 3,0 GHz Linux - 8 x Xeon de 3,0 GHz Solaris - V880 8 x Ultra Sparc III de 1,1 GHz

Sentinel Control Center Construtor de Coletor de Agente (somente no Windows) Gerenciador de Dados do Sentinel		
RAMEPS	**Espaço em RAM**	**CPU**
2 GB50	152 GB	Windows 2000, 2003 ou XP - 2 x Xeon de 3,0 GHz Windows XP (somente Control Center) - 2 x Xeon de 3,0 GHz SuSE Linux ou Redhat Linux - 2 x Xeon de 3,0 GHz Sun Solaris 9 - V280 2 x Ultra Sparc III de 1,1 GHz
500	2 GB	Windows 2000, 2003 ou XP Sun Solaris 9
1000+	4 GB	Windows 2000, 2003 ou XP Sun Solaris 9

Banco de Dados			
EPS	**RAM**	**Espaço**	**CPU**
250	8 GB	500 GB	Windows - 4 x Xeon de 3,0 GHz SuSE Linux ou Redhat Linux - 4 x Xeon de 3,0 GHz Solaris - V480 4 x Ultra Sparc III de 1,1 GHz
500	12 GB	1.0 TB	Windows - 4 x Xeon de 3,0 GHz SuSE Linux ou Redhat Linux - 4 x Xeon de 3,0 GHz Solaris - V880 6 x Ultra Sparc III de 1,1 GHz
1000+	16 GB	2.0 TB	Windows - 8 x Xeon de 3,0 GHz SuSE Linux ou Redhat Linux - 8 x Xeon de 3,0 GHz Solaris - V880 8 x Ultra Sparc III de 1,1 GHz

Configuração de matriz de disco

O servidor e-securityNovell Sentinel 5 em uma configuração de produção exige uma matriz de disco de alta velocidade para os hosts de Banco de Dados e do Sentinel. Esta seção tentará abordar as recomendações de configuração de disco (RAID) típicas. A seguir estão os principais componentes que são afetados pelo desempenho do hardware de Disco:

- Componente de banco de dados (MSSQL/Oracle): a taxa EPS (Events per Second) e os recursos de Consulta (desempenho de Consulta Rápida/Crystal) são afetados.
- DAS-RT (Data Access Service Real Time Component - Componente de Tempo Real de Serviço de Acesso a Dados): o recurso Tela Ativa é afetado.
- DAS-AggregationBinary (componente de Agregação): o número de resumos que podem ser ativados é afetado.

Requisito mínimo para instalação empresarial (1000 EPS ou mais)

No mínimo, é recomendável usar uma configuração RAID 5. A RAID 5 pode proporcionar a melhor relação custo/benefício. Essa configuração sacrifica parcialmente o desempenho e a redundância para reduzir o custo. Observe que estas são apenas recomendações, que devem ser usadas como guia. A maioria das instalações empresariais de produção em grande-escala exigirá uma análise mais detalhada dos requisitos de velocidade, throughput e redundância.

- Grupo RAID 1 – BD (Dados, Índices, registros de transação etc.)
- Grupo RAID 2 – DAS do Sentinel Server (diretório de Dados, DIR* Temporário)
- Mínimo de discos: 13 por Grupo RAID
- Tipo de disco: 12k+ RPM, Fiber Channel ou SCSI
- LUN 1 (Grupo RAID 1): 5GB – 144GB+ por disco
- LUN 2 (Grupo RAID 2): 5GB – 144GB+ por disco

Configuração otimizada

Para a obtenção de uma configuração com desempenho e redundância otimizados, uma RAID 1+0 pode ser utilizada com as mesmas configurações acima. No entanto, pode ser necessário ter Grupos RAID e LUNs adicionais que sigam as mesmas diretrizes acima para proporcionar maior paralelismo e E/S a determinados bancos de dados.

***NOTA**: Consulte a seção Instalando o Sentinel para obter instruções sobre como apontar o diretório DAS TEMP para um local diferente.

Exemplo de configuração Sstorage para uma instalação do MS SQL

Este exemplo usa o subsistema de armazenamento EMC^2 CLARiiON com:

- 1 TB de armazenamento
- 60 unidades, 36 GB, 15K RPM

Grupos RAID

Matriz	Grupo RAID	Número de unidades	Unidades designadas (barramento-invólucro-disco)	Nome
1	0	8	0-0-13, 0-0-14, 1-0-13, 1-0-14, 2-0-13, 2-0-14, 3-0-13, 3-0-13	Grupo RAID 0
1	1	8	0-0-11, 0-0-12, 1-0-11, 1-0-12, 2-0-11, 2-0-12, 3-0-11, 3-0-12	Grupo RAID 1
1	2	8	0-0-9, 0-0-10, 1-0-9, 1-0-10, 2-0-9, 2-0-10, 3-0-9, 3-0-10	Grupo RAID 2
1	3	8	0-0-7, 0-0-8, 1-0-7, 1-0-8, 2-0-7, 2-0-8, 3-0-7, 3-0-8	Grupo RAID 3
1	4	8	0-0-5, 0-0-6, 1-0-5, 1-0-6, 2-0-5, 2-0-6, 3-0-5, 3-0-6	Grupo RAID 4
1	5	8	0-0-3, 0-0-4, 1-0-3, 1-0-4, 2-0-3, 2-0-4, 3-0-3, 3-0-4	Grupo RAID 5
1	6	12	0-0-0, 0-0-1, 0-0-2, 1-0-0, 1-0-1, 1-0-2, 2-0-0, 2-0-1, 2-0-2, 3-0-0, 3-0-1, 3-0-2	Grupo RAID 6

Designações de LUN

Matriz	LUN	Tipo de RAID	Grupo RAID	Tamanho (GB)	Processador de armazenamento	Nome
1	0	0	0	263	A	LUN 0
1	1	0	1	263	B	LUN 1
1	2	0	2	263	A	LUN 2
1	3	0	3	263	B	LUN 3
1	4	0	4	263	A	LUN 4
1	5	0	5	214	B	LUN 5
1	6	0	6	160	A	LUN 6
1	7	0	6	160	B	LUN 7

Grupos de armazenamento

Matriz	Grupo de armazenamento	LUN	Host	Letra da unidade	Nome
1	Sentinel	0	E2P0 (E3P0)	E:	SQLData1
1	Sentinel	1	E2P0 (E3P0)	F:	SQLData2
1	Sentinel	2	E2P0 (E3P0)	G:	SQLData3
1	Sentinel	3	E2P0 (E3P0)	H:	SQLData4
1	Sentinel	4	E2P0 (E3P0)	I:	SQLIndex1
1	Sentinel	5	E2P0 (E3P0)	J:	SQLIndex2
1	Sentinel	6	E2P0 (E3P0)	L:	SQLLog
1	Sentinel	7	E2P0 (E3P0)	T:	TempDB

Exemplo de configuração de armazenamento para uma configuração do Oracle

volume 1	RAID 1	Home page da Oracle
volume 2	RAID 1	membro de redo log a
volume 3	RAID 1	membro de redo log b
volume 4	RAID 0+1 ou RAID 5	tablespaces undo e temp
volume 5	RAID 0+1 ou RAID 5	tablespaces de dados do e-SecuritySentinel
volume 6	RAID 0+1 ou RAID 5	tablespaces de índice do e-SecuritySentinel
volume 7	RAID 0+1 ou RAID 5	tablespaces de resumo do e-SecuritySentinel
volume 8	RAID 0+1 ou RAID 5	tablespaces de índice de resumo do e-SecuritySentinel
volume 9	RAID 1	arquivos de registro de arquivos

Configuração de rede

Componentes do Sentinel Server: Eles devem estar conectados uns aos outros por meio de um único switch de 1 GB. Isso inclui Banco de Dados, Servidor de Comunicação, Consultor, Serviços de Base do Sentinel, Mecanismo de Correlação e DAS.

Sentinel Control Center, Construtor de Coletor de Agente e Serviço Coletor de Agente (Gerenciador de Coletor de Agente): Eles precisam estar conectados a um Sentinel Server no mínimo por meio de switches FULL DUPLEX de 100Mbit.

Instalação do Oracle e MS SQL Server

NOTA: A maioria dos parâmetros de instalação de banco de dados pode ser mudada depois da instalação do banco de dados por meio do banco de dados ou da linha de comando.

1. Por motivos de desempenho, dependendo de se tratar da instalação em RAID, e se o ambiente RAID permitir, os registros a seguir devem ser instalados no disco de gravação mais rápido que estiver disponível.
   - Redo Log (Oracle)
   - Registro de Transação (MS SQL)
2. Para determinar com mais com precisão o tamanho do banco de dados, você pode começar com um banco de dados pequeno e aumentar o tamanho depois de utilizar o

sistema por um breve período. Isso lhe permitirá observar o crescimento do banco de dados com base na taxa de inserção de eventos para determinar os requisitos de espaço do banco de dados do sistema.

3. Para fins de recuperação, é recomendável executar backups programados regularmente do banco de dados.
4. Para instalações do Oracle, o instalador do Sentinel desativa o Registro de Arquivos por padrão. Para fins de recuperação de bancos de dados, é altamente recomendável que, após a instalação e antes de começar a receber dados de eventos de produção, você habilite o Registro de Arquivos. Você também deve programar um backup dos seus registros de arquivo para liberar espaço no destino do registro de arquivos, do contrário o banco de dados irá parar de aceitar eventos quando o destino de registro de arquivos atingir a capacidade completa.
5. Por motivos de desempenho, os locais de armazenamento devem apontar para locais diferentes, de modo a evitar contenções de E/S.
   - Diretório de dados
   - Diretório de índices
   - Diretório de Dados de Resumo
   - Diretório de Índices de Resumo
   - Diretório de Registro (Apenas MS SQL)
   - Diretório Temporário e Undo Tablespace: (Apenas Oracle)
   - Diretório A do Membro de Redo Log (Apenas Oracle)
   - Diretório B do Membro de Redo Log (Apenas Oracle)

Patches de banco de dados do e-SecuritySentinel

Apenas para MS SQL, w. Quando os patches de Banco de Dados do Sentinel são aplicados, o instalador apenas adiciona novos índices a *_P_MAX. As partições já existentes não serão atualizadas. Você precisará adicionar índices manualmente às partições já existentes se desejar que os novos índices aprimorem o desempenho para consultas executadas em relação às partições existentes.

Configurações recomendadas de Kernel UNIX

A seguir estão sugestões de valores mínimos. Para obter mais informações, consulte a documentação do sistema e do Oracle.

Valores de parâmetros de Kernel mínimos para Linux

Para obter mais informações sobre como exibir e definir parâmetros de kernel no Linux, consulte o *Capítulo 3 – Instalando o Sentinel 5 para Oracle – Pré-instalação do Oracle no Linux*.

```
shmmax=2147483648 (valor mínimo)
shmmni=4096
semmns=32000
semmni=1024
semmsl=1024
semopm=100
```

Valores de parâmetros de Kernel mínimos para Solaris

Verifique os parâmetros de kernel UNIX para Oracle em /etc/system e defina o seguinte:

```
shmmax=4294967295
shmmin=1
shmseg=50
shmmni=400
semmns=14000
semmni=1024
semmsl=1024
shmopm=100
shmvmx=32767
```

Parâmetros de configuração ao criar sua própria instância de banco de dados

A seguir estão as configurações recomendadas para a criação de sua própria instância de banco de dados. Suas configurações podem variar, dependendo da configuração e dos requisitos do sistema.

Na instância Oracle, será necessário criar:

- Parâmetros de inicialização Oracle (esses valores dependem do tamanho e da configuração do sistema)
- Tablespaces necessários do e-SecuritySentinel
- Parâmetros de configuração para Linux

Parâmetros Mínimos Recomendados para Configuração	
Parâmetros	**Tamanho (bytes ou outra especificação)**
db_cache_size	1 GB
java_pool_size	33.554.432
large_pool_size	8.388.608
shared_pool_size	100 MB
pga_aggregate_target	150.994.944
sort_area_size	109.051.904
open_cursors	500
cursor_sharing	SIMILAR
hash_join_enabled	TRUE
optimizer_index_caching	50
optimizer_index_cost_adj	55

Tamanho Mínimo Recomendado para Tablespace		
Tabela	**Tamanho de Exemplo**	**Notas**
REDO	3 x 100M	▪ Este é o valor mínimo. Você deve criar redo logs maiores se tiver um EPS elevado.
SYSTEM	500M	▪ Valor mínimo
TEMP	1G	▪ Valor mínimo
UNDO	1G	▪ Valor mínimo

Tamanho Mínimo Recomendado para Tablespace		
Tabela	**Tamanho de Exemplo**	**Notas**
ESENTD	5G	▪ Valor mínimo ▪ Este é para dados de eventos
ESENTD2	500M	▪ Valor mínimo ▪ Dados de configuração, bens, vulnerabilidade e associações (autoextend habilitado)
ESENTWFD	250M	▪ Para dados do iTraciTRAC (autoextend habilitado)
ESENTWFX	250M	▪ Para índice do iTraciTRAC (autoextend habilitado)
ESENTX	3G	▪ Valor mínimo ▪ Para índice de eventos
ESENTX2	500M	▪ Valor mínimo ▪ Índice de configuração, bens, vulnerabilidade e associações (autoextend habilitado)
SENT_ADVISORD	200M	▪ Valor mínimo ▪ Para dados do Advisor (autoextend habilitado)
SENT_ADVISORX	100M	▪ Valor mínimo ▪ Para índice do Advisor (autoextend habilitado)
SENT_LOBS	100M	▪ Valor mínimo ▪ Para objetos grandes de bancos de dados (autoextend habilitado)
SENT_SMRYD	3G	▪ Valor mínimo ▪ Para dados de resumo de Agregação
SENT_SMRYX	2G	▪ Valor mínimo ▪ Para índice de resumo de Agregação

Instalando o Sentinel

Quando o Sentinel é instalado, por motivos de desempenho e backup, os itens a seguir devem ser considerados.

1. Ao realizar uma instalação limpa do e-SecuritySentinel depois de ter uma versão anterior do e-SecuritySentinel instalada, é ALTAMENTE recomendável remover alguns arquivos e configurações do sistema dessa instalação anterior. Se esses arquivos não forem removidos, uma nova instalação limpa poderá falhar. Assim, uma nova instalação limpa poderá falhar. Esse procedimento deve ser realizado em cada máquina onde esteja sendo feita uma instalação limpa. Para obter mais informações sobre os arquivos que devem ser removidos, consulte o *Apêndice E*.

2. O desempenho de Telas Ativas e Mapeamento poderá ser bastante aprimorado se o diretório temp dos processos de DAS_RT e DAS_Query apontar para um disco rápido (por exemplo, uma matriz de disco). Para apontar o diretório temp dos processos para um disco rápido, faça o seguinte no computador em que o DAS está instalado:

   a. Crie um diretório no disco rápido para colocar nele os arquivos temporários. No UNIXSolaris, esse diretório deve pertencer e ser gravável pelo usuário esecadm e pelo grupo esec.

   b. Faça uma cópia de backup do arquivo %ESEC_HOME%\configuration.xml.

   c. Abra o arquivo %ESEC_HOME%\configuration.xml em um editor de texto.

   d. Para os processos DAS_RT e DAS_Query, adicione o argumento JVM java.io.tmpdir, definindo-o para o diretório que você acabou de criar.

   e. Para fazer essa mudança para o processo DAS_RT, procure a linha que contém o texto

```
-Dsrv_name=DAS_RT
```

   e adicione o argumento

```
-Djava.io.tmpdir=<tmp_directory>
```

   logo após ela. Um exemplo de como a linha deve ser (seus argumentos –Xmx, -Xms e –XX podem ter aparência diferente) é:

```
<process component="DAS"
   image="&quot;$(ESEC_JAVA_HOME)/java&quot; -server -
   Dsrv_name=DAS_RT -Djava.io.tmpdir=D:\Temp2 -Xmx310m
   -Xms103m -XX:+UseParallelGC -Xss128k -Xrs -
   Desecurity.dataobjects.config.file=/xml/BaseMetaDat
   a.xml -
   Djava.util.logging.config.file=../config/das_rt_log
   .prop -
   Dcom.esecurity.configurationfile=../../configuratio
   n.xml -
   Djava.security.auth.login.config=../config/auth.log
   in -Djava.security.krb5.conf=../../lib/krb5.conf -
   jar ../../lib/ccsbase.jar ..//config//das_rt.xml"
   min_instances="1" post_startup_delay="5"
   shutdown_command="cmd //C
   &quot;$(ESEC_HOME)/sentinel/scripts/stop_container.
   bat&quot; localhost DAS_RT"
   working_directory="$(ESEC_HOME)/sentinel/bin"/>
```

   f. Para fazer essa mudança para o processo DAS_Query, procure a linha que contém o texto

```
-Dsrv_name=DAS_Query
```

   e adicione o argumento

```
-Djava.io.tmpdir=<tmp_directory>
```

logo após ela. Um exemplo de como a linha deve ser (seus argumentos –Xmx, -Xms e –XX podem ter aparência diferente) é:

```
<process component="DAS"
   image="&quot;$(ESEC_JAVA_HOME)/java&quot; -server -
   Dsrv_name=DAS_Query -Djava.io.tmpdir=D:\Temp2 -
   Xmx256m -Xms85m -XX:+UseParallelGC -Xss128k -Xrs -
   Desecurity.dataobjects.config.file=/xml/BaseMetaDat
   a.xml,/xml/WorkflowMetaData.xml -
   Djava.util.logging.config.file=../config/das_query_
   log.prop -
   Djava.security.auth.login.config=../config/auth.log
   in -Djava.security.krb5.conf=../../lib/krb5.conf -
   Desecurity.execution.config.file=../config/executio
   n.properties -
   Dcom.esecurity.configurationfile=../../configuratio
   n.xml -jar ../../lib/ccsbase.jar
   ..//config//das_query.xml" min_instances="1"
   post_startup_delay="5" shutdown_command="cmd //C
   &quot;$(ESEC_HOME)/sentinel/scripts/stop_container.
   bat&quot; localhost DAS_Query"
   working_directory="$(ESEC_HOME)/sentinel/bin"/>
```

Maximizando a geração de relatórios para Crystal Reports

Dependendo do número de eventos que o Crystal estiver consultando, você poderá receber um erro sobre o tempo máximo de processamento ou o limite máximo de registros. Para definir o servidor para processar um número maior ou ilimitado de relatórios, será necessário reconfigurar o Crystal Page Server.

Reconfigurando o Crystal Page Server (apenas Windows Crystal Server)

1. Clique em *Iniciar* > *Todos os Programas* > *BusinessObjects 11* > *Crystal Reports Server* > *Central Configuration Manager*.
2. Clique o botão direito do mouse em *Crystal Reports Page Server* e selecione *Parar*.
3. Clique o botão direito do mouse em *Crystal Reports Page Server* e selecione *propriedades*.
4. No campo Comando, sob a guia Propriedades, ao final da linha de comando, adicione:

```
maxDBResultRecords <value greater than 20000 or 0 to
   disable the default limit>
```

5. Reinicie o *Crystal Page Server*.

Reconfigurando o Crystal Page Server (Servidores Linux ou Windows Crystal)

1. Abra um browser e digite este url:

   Para Servidores Linux Crystal:

   ```
   http://<DNS or IP of Crystal
      Server>:8080/businessobjects/enterprise11/adminlaun
      ch
   ```

   Para Servidores Windows Crystal:

   ```
   http://<nome DNS ou endereço IP do servidor
      Web>/businessobjects/enterprise11/WebTools/adminlau
      nch/default.aspx
   ```

2. Clique em *Central Management Console*.
3. O nome do sistema deve ser o nome do computador do host. O tipo de autenticação deve ser Enterprise. Caso contrário, escolha Enterprise.
4. Digite o nome do usuário e a senha e clique em *Log On*.
5. Clique em *Servers* (Servidores).
6. Clique em *<nome do servidor>.pageserver*.
7. Em *Database Records to Read When Previewing Or Refreshing a report* (Registros do Banco de Dados para Ler quando Visualizar ou Atualizar um Relatório), selecione *Unlimited records* (Registros ilimitados).
8. Clique em *Apply*.
9. Será exibido um prompt para reiniciar o servidor de página; clique em *OK*.
10. Talvez seja preciso fornecer um nome de logon e uma senha para acessar o gerenciador do serviço do sistema operacional.

Relatórios fornecidos com o Sentinel

1. Para a v5.1.1 SP1 e posterior, as 10 principais consultas de relatórios agregam tabelas em vez de uma tabela de eventos detalhados. Verifique se os serviços EventFileRedirectService e Aggregation (resumos) estão ativados.

   EventFileRedirectService está localizado na máquina DAS e ser habilitado mediante a edição de das_binary.xml.

   Os três resumos que precisam ser ativados são:

   - EventDestSummary
   - EventSevSummary
   - EventSrcSummary

   NOTA: Para obter informações sobre EventFileRedirectService e os três resumos de agregação, consulte o *Capítulo SDM no Guia do Usuário do Sentinel* ou os capítulos sobre a instalação do Crystal no *Guia de Instalação do Sentinel*.

2. Relatórios que consultam uma grande faixa de datas podem ter execução lenta. Eles devem ser programados em vez de ser executados interativamente.

   NOTA: Para obter informações sobre a programação do Crystal Reports, consulte a documentação do *Crystal BusinessObjects Enterprise™ 11*.

Dicas ao desenvolver Crystal Reports personalizados

Para relatórios personalizados desenvolvidos, é recomendável:

1. Utilizar o máximo possível de tabelas agregadas.
2. Se os relatórios puderem utilizar tabelas agregadas predefinidas, escolha a tabela agregada que resultar no processamento da menor quantidade de dados.
3. Tente to distribuir a maioria do processamento de dados para o mecanismo de banco de dados.
4. Para reduzir o overhead de processamento no Crystal Server, minimize a quantidade de dados para recuperar para o Crystal Server.

Melhores práticas de manutenção

Análise de banco de dados para Oracle

À medida que eventos são inseridos continuamente no banco de dados do Sentinel, as estatísticas do banco de dados devem ser atualizadas regularmente para garantir um bom desempenho de consulta.O Utilitário de Análise de banco de dados atualiza as estatísticas do banco de dados para dados de eventos no Oracle. Para a obtenção de um desempenho otimizado, esse utilitário deve ser programado para ser executado regularmente.

NOTA: Esse utilitário inclui um script SQL necessário que pode ser atualizado periodicamente. É recomendável verificar periodicamente o Portal do Cliente do e-SecurityNovell para determinar se há atualizações.

O seguinte script de shell deve ser executado regularmente por meio de cron ou outro programador:

- AnalyzePartitions.sh
- AnalyzeTables.sh

Analisar partições

O script AnalyzePartitions.sh analisa partições que foram preenchidas recentemente. Esse script deve ser programado diariamente para atualizar as estatísticas do banco de dados nas partições que são preenchidas a partir do dia anterior. É recomendável executar esse script duas horas depois da meia-noite quando eventos dos dias anteriores tiverem sido inseridos no banco de dados.

Esse script está localizado em $ESEC_HOME/utilities/db. Ele deve ser executado localmente no servidor em que o banco de dados do Sentinel está instalado. A conta de usuário UNIX que executa o script deve poder se conectar ao banco de dados como sysdba (por exemplo: oracle).

NOTA: Se tiver feito download de uma versão desse utilitário mais recente do que a versão instalada no momento no computador, você precisará instalar sp_esec_dba_utl.sql.

Instalando sp_esec_dba_utl.sql

1. Efetue login como proprietário do software Oracle.
2. Usando o SQL*Plus, conecte-se ao banco de dados como ESECDBA.
3. Instale o pacote ESEC_DBA_UTL. No prompt do SQL %(SQL>), digite:

```
@sp_esec_dba_utl.sql
```

4. Saia doSQL*Plus.

Executando AnalyzePartitions.shTo para executar este script:

1. Na máquina de servidor de banco de dados Oracle, execute o comando cd para:

```
$ESEC_HOME/utilities/db/
```

   ou execute o comando cd para o local de onde você fez o download do arquivo mais recente.
2. No prompt de comando, digite o seguinte:

   Para Solaris:

```
./AnalyzePartitions.sh <ORACLE_SID> >> <LogFileName>
```

   Para Linux:

```
ksh ./AnalyzePartitions.sh <ORACLE_SID> >>
   <LogFileName>
```

   - ORACLE_SID – o nome da instância do Oracle para o banco de dados.
   - LogFileName – o nome do caminho completo para o arquivo em que você deseja que as mensagens de registro sejam gravadas.

   Se o script for bem-sucedido, sairá com o código de retorno 0. Se falhar, sairá com p código de retorno 1. Programe seus trabalhos de maneira adequada para verificar o código de retorno. Se o trabalho de análise falhar, consulte o arquivo de registro para obter mensagens de erro detalhadas.

Verificação de saúde de banco de dados para Oracle

dbHealthCheck.sh é um script que reúne informações sobre o banco de dados do Sentinel Oracle. O script faz o seguinte:

- Verifica se a instância do banco de dados está ativada
- Verifica se a escuta do Oracle está ativada
- Exibe o uso do espaço
- Verifica se há índices não utilizáveis
- Verifica se há objetos inválidos do banco de dados
- Verifica se há análises do banco de dados

O script deve ser executado regularmente por meio de cron ou outro programador.

NOTA: Essa ferramenta de utilitário, incluindo um script SQL necessário, pode ser atualizada periodicamente. É recomendável verificar periodicamente o Portal do Cliente da Novell para determinar se há atualizações.

Instalando e executando dbHealthCheck.sh

NOTA: Se tiver feito download de uma versão desse utilitário mais recente do que a versão instalada no momento no computador, você precisará instalar sp_esec_dba_utl.sql.

Instalando sp_esec_dba_utl.sql

1. Efetue login como proprietário do software Oracle.
2. No servidor de banco de dados, verifique se $ORACLE_HOME e $ORACLE_SID estão definidos no ambiente.
3. Usando o SQL*Plus, conecte-se ao banco de dados como ESECDBA.
4. Instale o pacote ESEC_DBA_UTL. No prompt do SQL %(SQL>), digite:

```
@sp_esec_dba_utl.sql
```

5. Saia doSQL*Plus.

Executando dbHealthCheck.sh

NOTA: O script deve ser executado com uma conta de proprietário do software Oracle ou qualquer outra conta que possa se conectar "COMO SYSDBA"

NOTA: dbHealthCheck.sh deve ser executado localmente no servidor de banco de dados.

1. No servidor de banco de dados, verifique se $ORACLE_HOME e $ORACLE_SID estão definidos no ambiente.
2. Na máquina de Servidor de banco de dados Oracle, execute o comando cd para:

```
$ESEC_HOME/utilities/db/
```

   ou execute o comando cd para o local de onde você fez o download do arquivo mais recente.
3. No prompt de comando, digite o seguinte:

   Para Solaris:

```
./dbHealthCheck.sh
```

   Informações sobre o banco de dados do Sentinel serão exibidas na tela, ou você poderá gravar os resultados em um arquivo.

```
./dbHealthCheck.sh >> <filename>
```

   Para Linux:

```
ksh ./dbHealthCheck.sh
```

   Informações sobre o banco de dados do Sentinel serão exibidas na tela, ou você poderá gravar os resultados em um arquivo.

```
ksh ./dbHealthCheck.sh >> <filename>
```

Arquivando dados e adicionando partições automaticamente (apenas Windows)

NOTA: se sua máquina não tiver acesso ao DAS_Binary e DAS_Query, a Opção de Linha de Comando SDM pode ser usada no lugar da interface de usuário do SDM.

Este procedimento só é aplicável ao Windows. Garante que, durante a realização da sua pré-configuração e da configuração, seja realizado o seguinte:

- Certifique-se de que sdm.connect seja inicializado com a interface de usuário do SDM ou a linha de comando.
- Certifique-se de que o diretório de arquivo exista.
- Certifique-se de que os dias de archiveConfig e dropPartitions sejam iguais.
- Certifique-se de que o arquivo de lote seja corretamente executado do prompt de comando pelo menos uma vez antes de agendá-lo para execução automática.

NOTA: caso a tarefa agendada falhe, ela não envia uma notificação. A tarefa é registrada em SDM_*.log

Pré-configuração

Antes de configurar automaticamente Arquivar dados e Adicionar partições, você deve:

- Salvar propriedades de conexão
- Estabelecer parâmetros de arquivamento

Gravando as propriedades da conexão no Gerenciador de Dados do Sentinel

Este procedimento deve ser executado antes do uso das Opções de Linha de Comando do Gerenciador de Dados do Sentinel. Para gravar sua conexão (saveConnection) para o Gerenciador de Dados do Sentinel, você deve executar a Linha de Comando SDM com a ação saveConnection.

Se você tiver executado a interface de usuário do SDM, você usar o arquivo sdm.connect que foi criado com a interface de usuário. Ele está localizado em ESEC_HOME\sdm.

A ação saveConnection grava os detalhes da conexão em connectFile. O keystore ao qual é feita referência no arquivo configuration.xml é usado para criptografar a senha antes de gravá-la em connectFile.

As seguintes opções de linha de comando para a ação saveConnection estão disponíveis para definir os detalhes da conexão:

-action	saveConnection
-server	Mssql
-host	<endereço IP do host do banco de dados ou o nome de host ao qual se conectar>
-port	<número da porta do banco de dados ao qual se conectar [padrão SQL Server: 1433]>
-database	<nome/SID do banco de dados ao qual se conectar>
-user	<nome de usuário do banco de dados>
-password	<senha do banco de dados>
-winAuth	Usado para autenticação do Windows. Ao usar esta opção, não use –user e –password.
-connectFile	<nome de arquivo para gravar os detalhes de conexão [nome de arquivo de sua escolha]>

O aplicativo grava todos os detalhes de conexão acima junto com a senha criptografada no arquivo especificado. O aplicativo usa os detalhes gravados da conexão para executar as outras ações da linha de comando SDM. Essa etapa deve ser completada na primeira vez em que você iniciar o aplicativo e todas as vezes que desejar mudar os detalhes da conexão.

Executando saveConnection

1. Execute o comando como segue:

```
sdm -action saveConnection -server <oracle/mssql> -
   host <hostIp/hostName> -port <portnum> -database
   <databaseName/SID> [-driverProps <propertiesFile>]
   {-user <dbUser> -password <dbPass> | -winAuth} -
   connectFile <filenameToSaveConnection>
```

   O exemplo a seguir gravará os detalhes da conexão no arquivo sdm.connect para um banco de dados chamado esec em um host com o endereço IP 172.16.0.36 e a porta 1433 autenticado como usuário esecdba.

```
sdm -action saveConnection -server mssql -host
   172.16.0.36 -port 1433 -database esec -user esecdba
   -password XXXXXX -connectFile  sdm.connect
```

   O exemplo a seguir de Autenticação do Windows gravará os detalhes da conexão no arquivo sdm.connect para um banco de dados chamado esec_51 em um host com o endereço IP 172.16.1.3 e a porta 1433 autenticado usando a Autenticação do Windows.

```
sdm -action saveConnection -server mssql -host
   172.16.1.3 -port 1433 -database esec_51 –winAuth -
   connectFile  sdm.connect
```

Isso gravará os detalhes de conexão no arquivo sdm.connect. Todas as outras ações da linha de comando usarão esse nome de arquivo como entrada para se conectar ao banco de dados designado e executar suas ações.

NOTA: Se você tiver criado um arquivo connect para um local ou nome diferente daquele especificado no exemplo, precisará editar o arquivo manage_data.bat.

Estabelecendo os parâmetros de arquivamento

Pode-se fazer isso com a Linha de Comando SDM.

Esta ação %(archiveConfig) é usada para configurar o arquivamento. Esta configuração determina como os dados são arquivados das tabelas do Banco de Dados do e-SecuritySentinel.

Esta ação usa os seguintes indicadores:

-action	archiveConfig
-dirPath	<caminho válido de diretório no qual gravar os arquivos armazenados>
-keepDays	<número de dias a serem mantidos>
-connectFile	<caminho para o nome de arquivo gravado por "saveConnection">

Estabelecendo parâmetros de arquivamento através da Linha de Comando

1. Crie um diretório de saída de arquivo na raiz chamada SDM_archive %(c:\SDM_archive).

   NOTA: se criar um diretório de saída ou local diferentes, você terá que editar o arquivo manage_data.bat.

2. Execute este comando da seguinte forma:

```
sdm -action archiveConfig  -dirPath <caminho de
   diretório no qual gravar os arquivos armazenados> -
   keepDays <número de dias a serem mantidos> -
   connectFile <caminho para o nome de arquivo gravado
   por "saveConnection">
```

   O exemplo a seguir arquiva todos os dados mais antigos do que 30 dias no diretório c:\SDM_archive.

```
sdm -action archiveConfig –dirpath c:\SDM_archive -
   keepDays 30 -connectFile sdm.connect
```

Estabelecendo parâmetros de arquivamento através da interface de usuário

1. Crie um diretório de saída de arquivo na raiz chamada SDM_archive %(c:\SDM_archive).

   NOTA: se criar um diretório de saída ou local diferentes, você terá que editar o arquivo manage_data.bat.

2. A interface de usuário do SDM não exige parâmetros de arquivamento. A interface de usuário pode arquivar diretamente os dados sem precisar estabelecer parâmetros de arquivamento.

Apagar dados %(eliminar partições)

Esta ação (deleteData) apaga os dados mais antigos do que "keepDays" das tabelas a seguir:

- EVENTS
- CORRELATED_EVENTS

Por padrão, esta ação não descarta nenhuma partição que não está arquivada. Se desejar apagar as partições não-arquivadas, o indicador opcional "forceDelete" precisa ser especificado com um valor de verdadeiro. Caso se use forceDelete:

falso ou não especificado	descarta apenas as partições arquivadas mais antigas do que keepDays. Não apaga partições não arquivadas, mesmo que elas sejam mais antigas do que keepDays.
verdadeiro	elimina todas as partições mais antigas do que keepDays, incluindo as partições não-arquivadas

Este comando usa os seguintes indicadores:

-action	deleteData
-keepDays	<número de dias a serem mantidos>
[-forceDelete]	<verdadeiro ou falso>
-connectFile	<caminho para o nome de arquivo gravado por "saveConnection">

Executando deleteData

1. Execute este comando da seguinte forma:

```
sdm -action deleteData -keepDays <número de dias a
   serem mantidos> -connectFile <caminho para o nome
   de arquivo gravado por "saveConnection">
```

O exemplo a seguir elimina as partições das tabelas EVENTS e CORRELATED_EVENTS que são mais antigas do que 30 dias, garantindo que todas as partições descartadas sejam arquivadas. No final, lista todas as partições que não foram apagadas caso não tenham sido arquivadas.

```
sdm -action deleteData -keepDays 30 -connectFile
   sdm.connect
```

Programando arquivamento de dados e adicionando partições

NOTA: O arquivo manage_data.bat é configurado para um valor de keepDay de 30, para uma saída de arquivo para c:\SDM_archive e para um arquivo de conexão ESEC_HOME\SDM\sdm.connect.Caso seus valores sejam diferentes, você precisará editar o arquivo manage_data.bat.

Se você tiver definido as propriedades da sua conexão e os parâmetros de arquivamento, execute manage_data.bat do prompt de comando para garantir que esteja funcionando.

Para arquivar dados e adicionar partições automaticamente

NOTA: As etapas a seguir são para o Windows 2000 Professional. As etapas para o Windows 2000 Server, XP e 2003 podem ser diferentes, embora semelhantes.

1. No Windows, clique em *Iniciar* > *Configuração* > *Painel de controle*.
2. Clique duas vezes em *'Tarefas Agendadas'*.
3. Clique duas vezes em *'Adicionar Tarefa Agendada'*. Clique em *Avançar*.
4. Clique no botão *Procurar* e vá até o arquivo manage_data.bat %(ESEC_HOME\sdm).
5. Dê um nome para a tarefa agendada, como SDM_Archive. Selecione Diariamente em *'Realizar esta tarefa*:'. Clique em *Avançar*.
6. Selecione uma hora do dia para executar esta tarefa. Clique em *Avançar*.
7. Insira uma hora e uma data de sua preferência. Clique em *Avançar*.

8. Insira um nome com o qual esta tarefa será executada. O usuário não pode ser a conta de sistema local. Deve ser executado como usuário específico. Se estiver usando a Autenticação do Windows para se conectar ao banco de dados, você deverá usar o Usuário do Windows de Administrador de Banco de Dados do e-SecuritySentinel. Clique em *Avançar*.
9. Clique em *Concluir* para encerrar como tarefa agendada.

Mecanismo de Correlação

NOTA: Para que o Mecanismo de Correlação do Sentinel funcione corretamente, o horário da máquina do sistema precisa ser sincronizado dentro de ± 30 segundos de todas as máquinas do Gerenciador de Coletor. É recomendável que todas as máquinas do Mecanismo de Correlação e do Gerenciador de Coletor sejam conectadas a um Servidor NTP %(Network Time Protocol) ou outro tipo de Servidor de horário.

Entendendo regras de correlação avançadas

A regra de correlação avançada é usada para detecar relacionamentos entre eventos, como quando um evento específico ocorre (evento B) depois do evento A com um relacionamento entre os dois eventos. Nesse caso, o evento B é o evento atual e deve ser identificado com um filtro que você digita no painel do assistente de Critérios de Filtro de Eventos. O evento A é o evento passado e deve ser identificado com um filtro que você digita no painel de assistente de Critérios de Filtro de Eventos Passados. O relacionamento entre os dois eventos (ou seja, eles têm o mesmo endereço IP de origem e de destino) deve ser digitado no painel assistente de Critérios de Eventos versus Eventos Passados. Neste painel, você também especifica o tempo máximo entre os dois eventos que você deseja detectar; esta é a janela de tempo.
Se um evento passar em todos esses critérios, poderá ser agrupado e contado até um valor limite indicado no painel assistente de Critérios de Limite e Agrupamento.

Tempo de controle

As operações de Janela e Acionador têm uma janela de tempo associada a elas. Quanto maior for a janela de tempo, mais eventos (na verdade, informações de eventos) poderão ser armazenados na memória para essa janela de tempo. Para a operação de Janela, o que é armazenado depende do filtro especificado para os eventos passados. Quanto mais específico esse filtro puder ser, menos eventos serão armazenados na janela de tempo, permitindo que um período de tempo hora seja usado (se necessário). Para a operação de Acionador, o espaço máximo de armazenamento total que pode ser usado depende da cardinalidade do discriminador (ou seja: quanto mais agrupamentos possíveis houver, mais eventos poderão ser armazenados com o passar do tempo) até a quantidade limite para cada grupo. Muitas vezes, a redução do limite e do período de tempo para a operação de Acionador produzirá resultados equivalentes.

Entendendo a atualização de acionador

Suponha que você tenha recebido um evento correlacionado para uma regra, mas espere mais eventos correlacionados. Isso pode ocorrer devido ao comportamento de atualização da operação de Acionador. Na operação de Acionador, você pode especificar que quando houver um conjunto de 'n' eventos durante o período de tempo de 't', deverá ser acionado um evento correlacionado. Sempre que o mecanismo de correlação encontrar esse conjunto de 'n' eventos durante o período de tempo de 't', ocorrerá o acionamento. Se, durante o acionamento, for determinado que ele ocorreu anteriormente (para o mesmo agrupamento) e houver pelo menos um membro do conjunto em comum, esses membros serão adicionados ao evento correlacionado original em vez de criar um novo evento correlacionado.

Análise de curto-circuito de suporte a expressões booleanas

As comparações numéricas são mais rápidas do que comparações de string e as comparações de string são mais rápidas do que as comparações de expressões regulares. A operação dfe Filtro executa uma análise de curto-circuito nas expressões Booleanas. Ordenando cuidadosamente sua expressão, você pode tornar a avaliação mais rápida.

Não tenha medo do formato livre

Se você não puder expressar uma regra de correlação usando os três gabaritos predefinidos do assistente (Lista de Avisos, Básico ou Avançado), não tenha receio de construir uma regra de formato livre. Todos os gabaritos terminam por formar uma regra de formato livre para o usuário. Você pode ver a representação de formato livre editando a regra e mudando seu tipo para formato livre. Essa pode ser uma maneira fácil de estender uma regra que você não pôde expressar totalmente usando uma das três outras opções.

Registro de transações

Para o SQL Server, por padrão, os bancos de dados do Sentinel são criados de acordo com o modelo de recuperação completa. Segundo esse modelo, o espaço usado do Registro de Transações só é liberado depois que um backup do Registro de Transações é executado. Para impedir que o Registro de Transações fique cheio, os backups do registro devem ser programados no SQL Server ao longo do dia (3 a 4 vezes por dia, dependendo da taxa de eventos). Se a sua organização não necessitar da capacidade de executar a recuperação de ponto de falha, você poderá comutar o modelo de recuperação de banco de dados para simples. Segundo o modelo simples de recuperação de banco de dados, o espaço do Registro de Transações será liberado automaticamente pelo SQL Server, sem quaisquer backups do registro.

Locais do arquivo de registro do Sentinel

Há determinados registros no Sentinel que são úteis para a solução de problemas do sistema. Esses registros podem ser extremamente úteis quando você trabalha com o Suporte Técnico do e-SecurityNovell ao tentar resolver problemas.

Gerenciador de Dados do Sentinel

Registra atividades executadas usando o Gerenciador de Dados do Sentinel para o cliente específico executado no computador.

Para Windows:

```
ESEC_HOME\sdm\SDM_*.0.log
```

Para UNIX:

```
$ESEC_HOME/sdm/SDM_*.0.log
```

iTRAC

Registra atividades relacionadas ao iTRAC.

Para Windows:

```
ESEC_HOME\sentinel\log\das_itrac_0.*.logESEC_HOME\sent
   inel\log\das_itrac_0.*.log
```

Para UNIX:

```
$ESEC_HOME/sentinel/log/das_itrac_0.*.log
```

Consultor

Registra atividades relacionadas ao download e processamento de dados do Consultor.

Para Windows:

```
ESEC_HOME\sentinel\log\advisor.log
ESEC_HOME\sentinel\log\Advisor_0.*.log
```

Para UNIX:

```
$ESEC_HOME/sentinel/log/advisor.log
$ESEC_HOME/sentinel/log/Advisor_0.*.log
```

Inserção de eventos

Registra atividades relacionadas à inserção de eventos no banco de dados.

Para Windows:

```
ESEC_HOME\sentinel\log\das_binary0.*.log
```

Para UNIX:

```
$ESEC_HOME/sentinel/log/das_binary0.*.log
```

Consultas de banco de dados

Registra atividades relacionadas a consultas de banco de dados, agentCollector, saúde do gerenciador do agentCollector e todas as outras atividades do DAS não executadas por outros componentes do DAS.

Para Windows:

```
ESEC_HOME\sentinel\log\das_query0.*.log
```

Para UNIX:

```
$ESEC_HOME/sentinel/log/das_query0.*.log
```

Telas Ativas

Registra atividades relacionadas a Telas Ativas.

Para Windows:

```
ESEC_HOME\sentinel\log\das_rt0.*.log
```

Para UNIX:

```
$ESEC_HOME/sentinel/log/das_rt0.*.log
```

Agregação

Registra atividades relacionadas a agregação.

Para Windows:

```
ESEC_HOME\sentinel\log\das_aggregation0.*.log
```

Para UNIX:

```
$ESEC_HOME/sentinel/log/das_aggregation0.*.log
```

Watchdog do Sentinel

Registra atividades relacionadas ao Sentinel Watchdog.

NOTA: sentinel_wrapper.log refere-se ao agrupador de serviço.

Para Windows:

```
ESEC_HOME\sentinel\log\sentinel0.*.log
ESEC_HOME\sentinel\log\sentinel_wrapper.log
```

Para UNIX:

```
$ESEC_HOME/sentinel/log/sentinel0.*.log
$ESEC_HOME/sentinel/log/sentinel_wrapper.log
```

Gerenciador do AgentCollector

Registra atividades relacionadas ao Gerenciador do AgentCollector.

NOTA: agent-manager.log refere-se ao agrupador de serviço.

Para Windows:

```
ESEC_HOME\wizard\logs\agent-manager.log
ESEC_HOME\wizard\logs\am0.*.log
```

Para UNIX:

```
$ESEC_HOME/wizard/logs/agent-manager.log
$ESEC_HOME/wizard/logs/am0.*.log
```

3 Instalando o Sentinel 5 para Oracle no Solaris

NOTA: O termo Agente é sinônimo de Coletor. De agora em diante, Agentes serão referidos como Coletores.

Este capítulo descreve a instalação do Sentinel Enterprise Security Management Sentinel 5 para Oracle no Solaris.

Pré-instalação do Sentinel 5 para Oracle no Solaris

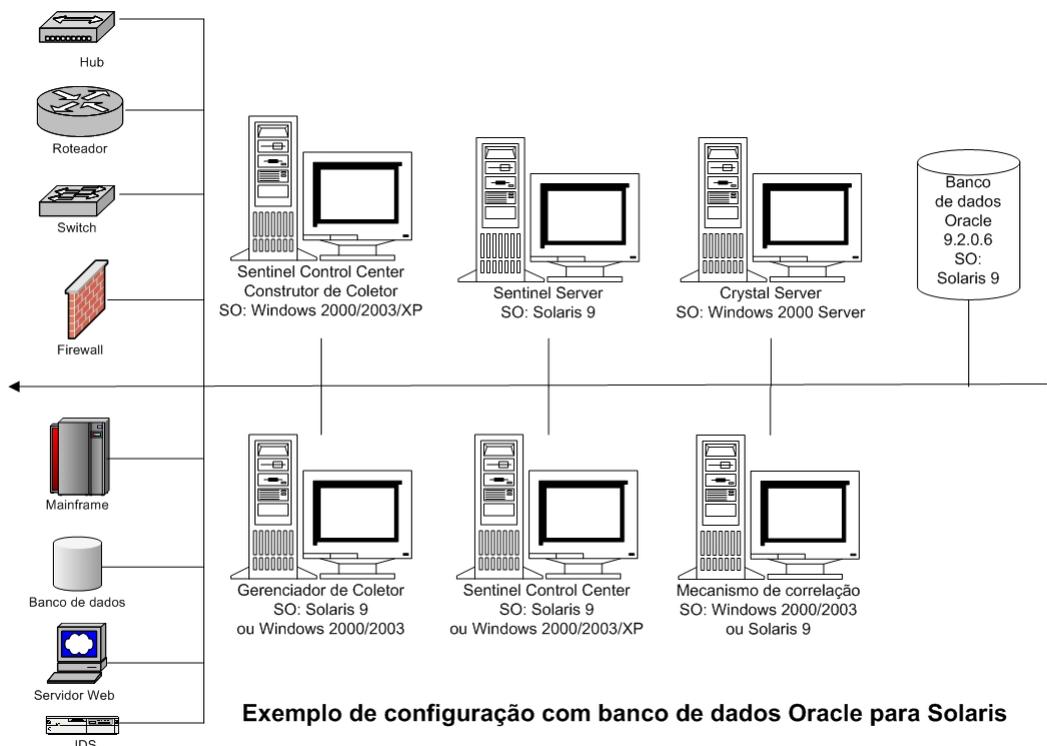
NOTA: Antes da instalação, assegure-se de que as máquinas atendem aos requisitos mínimos do sistema e que o sistema operacional foi "reforçado" com o uso das melhores práticas de segurança atuais.

NOTA: Instale o Oracle Enterprise com particionamento. O Gerenciador de Dados do Sentinel precisa desse recurso para gerenciar o Banco de dados do Sentinel.

NOTA: Ao realizar uma instalação limpa do Sentinel depois de ter uma versão anterior do Sentinel instalada, é necessário remover alguns arquivos e configurações do sistema que podem ter sobrado de uma instalação anterior. Se esses arquivos ou configurações não forem removidos, uma nova instalação limpa pode falhar.
Esse procedimento deve ser realizado em cada máquina onde esteja sendo feita uma instalação limpa. Para obter mais informações, veja o *Apêndice E*.

A seguir estão configurações típicas do Solaris para Sentinel. A configuração pode ser diferente dependendo do ambiente. Independentemente da configuração escolhida, é necessário instalar o banco de dados primeiro.

Exemplo de configuração com banco de dados Oracle para Solaris

---

NOTA: Para obter mais informações sobre os sistemas operacionais suportados, consulte o *Capítulo 1 – Introdução, Plataformas Suportadas para o Sentinel Server no Solaris.*

Obtendo uma Chave de Licença

O Serviço de Banco de Dados (DAS) do Sentinel Server requer uma chave de licença válida para instalar e executar o serviço. Essa chave de licença fica bloqueada na máquina onde o DAS será instalado. Uma chave de licença emitida para uma máquina não funciona em outra máquina.

Para obter a chave de licença, é necessário determinar o número de ID do host e fornecer essas informações para a Novell, que fornecerá uma chave de licença.

Para determinar o ID de host (Solaris)

1. Digite o seguinte comando:

```
hostid
```

2. Envie esse número de ID do host para o Suporte Técnico da Novell. Eles fornecerão a você uma chave de licença.

Banco de Dados do Sentinel

Antes de instalar o Banco de Dados do Sentinel, será necessário o seguinte:

- Para saber quais são os requisitos de hardware, consulte os *Capítulos 1 e 2*.
- Sun SPARC Solaris Server em execução no Solaris 9 com o Patch Cluster DATE recomendado: 03/05/05

- Oracle 9i Enterprise Edition 9.2.0.6 ou 9.2.0.7 com particionamento
- Para o Solaris, uma cópia do Oracle Note: 148673.1 SOLARIS: Guia de Inicialização Rápida
- Usuário do sistema operacional Oracle (padrão: oracle)
- Verifique se as seguintes variáveis de ambiente estão definidas para o usuário do sistema operacional Oracle:
    - ORACLE_HOME
    - ORACLE_BASE
    - PATH (é preciso ter $ORACLE_HOME/bin)
    - Embora não seja recomendado, se você criar manualmente a instância de banco de dados Oracle, consulte Criando uma Instância Oracle para o Banco de Dados Sentinel para ver instruções sobre a criação da instância Oracle. Caso você escolha essa opção, ainda será necessário usar o instalador para adicionar os objetos do banco de dados à instância de banco de dados Oracle recém criada (consulte Instalação Personalizada).

NOTA: Caso esteja usando uma instância de banco de dados Oracle existente ou criada manualmente, ela precisa estar vazia, exceto pela presença do usuário esecdba.

- Se estiver usando o instalador para criar a instância de banco de dados Oracle (recomendável), serão necessários os caminhos de diretório para colocar os arquivos de banco de dados. Esses diretórios precisam já existir antes da execução do instalador já que ele não cria esses diretórios. Esses diretórios também precisam permitir gravação pelo usuário do sistema operacional Oracle (p. ex. – oracle).

NOTA: Por motivos de desempenho, dependendo de se tratar da instalação em RAID, e se o ambiente RAID permitir, o Redo Log deve apontar para o disco de gravação mais rápido que estiver disponível.

NOTA: Por padrão, o instalador define que as seguintes tabelas NÃO devem crescer automaticamente: ESENTD, ESENTX, SENT_SMRYD e SENT_SMRYX. Fica definido o crescimento automático de todas as outras tabelas. O motivo para não permitir o crescimento automático das tabelas ESENTD, ESENTX, SENT_SMRYD e SENT_SMRYX é que elas contêm dados de eventos e dados resumidos de eventos. A utilização do espaço para eventos e resumos pode ser altamente dinâmica. Essas tabelas de eventos devem ser monitoradas e estendidas de forma controlada, com base na configuração do sistema de arquivos e levando em consideração o equilíbrio de E/S e o backup e recuperação de bancos de dados.

O gerenciamento de partições SDM (arquivamento, descarte e adição de partições) deve ser programado de modo a manter os dados do evento em tamanho controlado.

Sentinel Server

NOTA: Se o Banco de Dados do Sentinel não for instalado ao mesmo tempo em que o Sentinel Server, será necessário instalar o Banco de Dados do Sentinel primeiro.

Antes de instalar o Sentinel Server, será necessário:

- Para saber quais são os requisitos de hardware, consulte os *Capítulos 1 e 2*.
- Sun SPARC Solaris Server em execução no Solaris 9 com o Patch Cluster DATE recomendado: 03/05/05

- Número de série e Chave de licença do Sentinel 5 (Para DAS). Para obter mais informações, consulte Obtendo uma Chave de Licença.
- Servidor SMTP – Necessário para o envio de e-mails do Sentinel.

Sentinel Control Center e Assistente

Antes de instalar o Sentinel Server, será necessário:

- Para obter os requisitos de hardware, consulte os *Capítulos 1 e 2*
- Um dos seguintes sistemas operacionais:
  - Sun SPARC Solaris Server em execução no Solaris 9 com o Patch Cluster DATE recomendado do Solaris 9: May/03/05patches
  - (Construtor de Coletor somente) – Windows 2000 ou 2003

Consultor

Para instalar o Advisor, será necessário obter um ID e senha do Advisor com o Sentinel. O Download Direto da Internet usa a porta 443.

NOTA: Caso pretenda usar o Advisor para o Exploit Detection somente, não é necessário instalar o software Crystal Enterprise. Isso só é obrigatório se a intenção for executar Crystal Reports para Sentinel. Consulte o Capítulo 8, Configuração do Consultor, para obter mais informações.

Verificando o Layout do Solaris (Requisitos de Patch do Sistema Operacional)

Verificando o Layout do Solaris

1. Vá até o site da Sun na Internet e faça o download do conjunto de patches recomendado para o Solaris 9:
   - Patch Cluster DATE: 03/05/05

   NOTA: Consulte o arquivo README e a documentação adicional incluída.
   É ALTAMENTE recomendável que um backup completo do sistema seja feito antes da aplicação de patches.
2. Efetue login como Usuário Root e instale o cluster de patches aplicável e os patches de kernel.
3. Após a conclusão dos patches, apague o arquivo *_Recommended.zip e os arquivos estendidos contidos nos diretórios criados pelo patch e reinicialize o servidor.

Pré-instalação do Oracle no Solaris

Para a instalação do Oracle no Solaris para Sentinel, as seguintes ações são necessárias:

- Definição de valores de kernel
- Criação de uma conta de grupo e de usuário do Oracle
- Definição de variáveis de ambiente
- Instalação do Oracle 9.2.0.6 ou 9.2.0.7
- Aplicação do patch do Oracle 9.2.0.6 ou 9.2.0.7

Definindo os valores de Kernel para o Oracle no Solaris

Para a instalação do Oracle no Solaris, os seguintes valores de kernel têm de ser definidos em /etc/system.

ISENÇÃO DE RESPONSABILIDADE: A seguir estão sugestões de valores mínimos. Consulte o administrador do sistema e a documentação do Oracle para obter mais informações.

- shmmax=4294967295
- shmmin=1
- shmseg=50
- shmmni=400
- semmns=14000
- semmni=1024
- semmsl=1024
- shmopm=100
- shmvmx=32767

NOTA: Se os valores de kernel forem iguais ou maiores que os requisitos acima, não será necessário mudar as configurações.

1. Efetue login como Usuário Root.
2. Faça uma cópia de backup de /etc/system
3. Usando um editor de texto, mude as configurações do parâmetro de kernel no arquivo /etc/system conforme a tabela acima.
4. Reinicialize.

Pré-instalação do Oracle no Solaris

ISENÇÃO DE RESPONSABILIDADE: As instruções a seguir não têm por objetivo substituir a documentação do Oracle. Trata-se apenas de um exemplo de cenário de configuração. Esta documentação supõe que o diretório pessoal dos usuários do Oracle é /export/home/oracle e que o Oracle será instalado em /opt/oracle. A configuração exata pode variar. Consulte a documentação do sistema operacional e do Oracle para obter mais informações.

NOTA: Ao instalar o software Oracle, recomenda-se a escolha da instalação "típica". Caso contrário, ao fazer a instalação personalizada, escolha a instalação da Interface Oracle JDBC/OCI. Para obter mais informações, consulte a documentação do Oracle.

1. Efetue login como Usuário Root.
2. Crie um grupo UNIX e uma conta de usuário UNIX para o proprietário do banco de dados Oracle.

   Adicione um grupo dba (como root):

   ```
   groupadd –g 400 dba
   ```

   Adicione o usuário do Oracle (como root):

   ```
   useradd –g dba –d /export/home/oracle –m –s /bin/csh
      oracle
   ```

3. Para definir as variáveis de ambiente necessárias para o Oracle, sugerimos adicionar as seguintes informações ao arquivo local.cshrc:

   ```
   umask 022
   setenv ORACLE_HOME /opt/oracle
   ```

```
setenv ORACLE_SID ESEC
setenv LD_LIBRARY_PATH ${ORACLE_HOME}/lib
setenv DISPLAY :0.0
definir caminho=(/bin /bin/java /usr/bin /usr/sbin
   ${ORACLE_HOME}/bin /usr/ucb/etc.)
se ( $?prompt ) então
definir histórico=32
endif
```

4. Complete as etapas descritas no Oracle Note: 148673.1 SOLARIS: Guia de Inicialização Rápida.
5. Instale o Oracle 9i Release 2 como usuário do Oracle. Serão solicitados dois CD-ROMs adicionais. Você precisará navegar até diferentes diretórios para cada um dos CD-ROMs adicionais.
6. Aplique ao sistema o patch para o release 9.2.0.6.0 ou 9.2.0.7.0. Consulte a documentação do Oracle para obter os procedimentos de patch.
7. Para verificar o nível de patch, como o usuário do Oracle UNIX, digite:

   ```
   sqlplus '/as sysdba'
   ```

   Os resultados devem indicar um release de 9.2.0.6.0 ou 9.2.0.7.0. Digite quit para sair.
8. Remova o diretório criado para o patch.
9. Depois de instalar os patches, remova os diretórios e arquivos dos patches.
10. Reinicialize.

Instalação do Sentinel 5 para Oracle no Solaris

O Sentinel 5 dá suporte a dois tipos de instalação. São elas:

- Simples – Opção de instalação da all-in-one. Serviços do Sentinel, Serviço do Coletor e Aplicativos do Oracle na mesma máquina. O tipo de instalação se destina a fins demonstrativos apenas.
- Personalizado – Permite uma instalação totalmente distribuída.

Instalação Simples no Solaris

Essa opção instala os componentes mais comuns (não inclui o Construtor de Coletor nem recursos de Integração de Terceiros) em uma única máquina. Se destina principalmente a fins demonstrativos. Não é recomendada para uso em um ambiente de teste ou produção.

NOTA: A instalação simples não oferece suporte à autenticação de senha do Gerenciador de Coletor.

Como realizar uma Instalação Simples

1. Verifique se você coletou as informações, realizou as tarefas e atendeu aos requisitos especificados na seção Pré-instalação do Sentinel 5 para Oracle em relação aos componentes que está instalando.
2. Verifique a configuração do Oracle no Solaris.

3. Faça login como usuário Root.
4. Insira e monte o CD de instalação do Sentinel.
5. Para iniciar o programa de instalação, vá para o diretório de instalação no CD-ROM e digite:

   Para o modo de interface gráfica:

   ```
   ./setup.sh
   ```

   ou

   Para modo textual:

   ```
   ./setup.sh –console
   ```

6. Clique na seta para baixo e selecione uma das seguintes opções de idioma:
   - Inglês.
   - Francês
   - Alemão
   - Italiano
   - Português
   - Espanhol
7. Siga os prompts do instalador.
8. Depois de ler a tela de boas-vindas, clique em *Avançar*.
9. Aceite o Contrato de Licença de Usuário Final e clique em *Avançar*.
10. Aceite o diretório de instalação padrão ou clique em *Procurar* para especificar o local da instalação. Clique em *Avançar*.

    Nome do directório:
    /opt/sentinel5.1.3.0
    Procurar

11. Selecione *Simples*. Clique em *Avançar*.

12. Digite as informações sobre a configuração.
    - Número de Série e Chave de Licença
    - Servidor SMTP (o nome DNS ou o endereço IP) – essa opção permite ao Sentinel enviar e-mails.
    - Email – digite um endereço de e-mail válido para o qual os e-mails de notificação do Advisor devem ser enviados (p.ex. - Sent_Server@myserver.com).
    - Senha Global do Sistema – digite uma senha e a senha de confirmação correspondente. Esta será a senha de todos os usuários padrão. Isso inclui o usuário do sistema operacional esecadm e os usuários dos bancos de dados. Consulte o Banco de Dados do Sentinel, na seção Pós-instalação do Sentinel 5 para Oracle, para obter a lista de usuários padrão do banco de dados criada durante a instalação.

- Diretório de Dados – o local de todos os arquivos de dados para download do Banco de Dados e do Advisor (caso esteja instalando o Advisor). Para mudar o local padrão, clique no botão ... e selecione um local. O padrão é $ESEC_HOME/data.

NOTA: O Diretório de Dados precisa ficar acessível (para leitura, gravação e execução) ao usuário do Oracle e ao usuário esecadm. Como essa instalação é para fins demonstrativos apenas, é recomendado que essa acessibilidade seja alcançada tornando o Diretório de Dados legível, gravável e executável por todos. Para isso, execute o comando a seguir:

chmod 777 <caminho_do_diretório>

NOTA: Se estiver instalando o Advisor, a opção de instalação Simples irá configurar o Advisor para que use o Download Direto da Internet com um intervalo de atualização de 12 horas e todas as notificações de e-mail habilitadas.

- Para instalar o Advisor, selecione *Instalar Consultor*. Digite um nome de usuário e senha. Se o nome de usuário ou senha não puder ser verificado, após clicar em *Avançar* você será perguntado se deseja continuar (não recomendado). Se optar por continuar, digite a senha do Advisor novamente na janela de confirmação de senha. Caso contrário, corrija a senha do Advisor.

Clique em *Avançar*.

Número de Série:
Chave de Licença:
Servidor SMTP: localhost
E-mail: esecadm
Senha Global do Sistema (usada para todos os usuários do Sentinel e o Gerenciador de Coletor)
Senha:
Confirmar Senha:
Diretório de Dados: /opt/sentinel5.1.3.0/data
...
Instalar Consultor (digite o nome de usuário/senha abaixo)
Nome de Usuário:
Senha:

13. Digite as informações sobre a configuração do banco de dados:
    - Nome do Banco de Dados – O nome da instância de banco de dados Oracle para a criação e instalação de objetos do Banco de Dados do Sentinel. Não pode já existir um banco de dados com esse nome.
    - Arquivo de Driver do Oracle JDBC. Esse é o caminho completo para o arquivo .jar, normalmente $ORACLE_HOME/jdbc/lib/ojdbc14.jar (não é possível usar variáveis de ambiente nesse campo).

14. Clique em *OK* no nome de usuário do Oracle padrão.

15. Leia as informações apresentadas nas telas que aparecerem e clique em *Avançar* ao concluir. Depois de concluída a instalação, será necessário reinicializar o sistema.

NOTA: Caso deseje instalar algum software de Integração de Terceiros (Suporte técnico HP ou Integração do Remedy), após a reinicialização da máquina, execute o instalador novamente e selecione o software de Integração de Terceiros a ser instalado. Para obter mais informações, consulte o *Guia de Integração de Terceiros*.

---

16. O instalador do Sentinel desliga o Registro de Arquivos por padrão. Para fins de recuperação de bancos de dados, é altamente recomendável que, após a instalação e antes de começar a receber dados de eventos de produção, você habilite o Registro de Arquivos. Você também deve programar um backup dos seus registros de arquivo para liberar espaço no destino do registro de arquivos, do contrário o banco de dados irá parar de aceitar eventos.

Instalação Personalizada no Solaris

Como realizar uma Instalação Personalizada

1. Verifique se você coletou as informações, realizou as tarefas e atendeu aos requisitos especificados na seção Pré-instalação do Sentinel 5 para Oracle em relação aos componentes que está instalando.
2. Verifique a configuração do Oracle no Solaris.
3. Faça login como usuário Root.
4. Insira e monte o CD de instalação do Sentinel.
5. Para iniciar o programa de instalação, vá para o diretório de instalação no CD-ROM e digite:

   Para o modo de interface gráfica:

   ```
   ./setup.sh
   ```

   ou

   Para modo textual:

   ```
   ./setup.sh –console
   ```

6. Clique na seta para baixo e selecione uma das seguintes opções de idioma:

▪	Inglês	▪	Italiano
▪	Francês	▪	Português
▪	Alemão	▪	Espanhol

7. Depois de ler a tela de boas-vindas, clique em *Avançar*.
8. Aceite o Contrato de Licença de Usuário Final e clique em *Avançar*.
9. Aceite o diretório de instalação padrão ou clique em *Procurar* para especificar o local da instalação. Clique em *Avançar*.

10. Selecione *Personalizado* (padrão). Clique em *Avançar*.
11. Selecione os recursos a serem instalados.

NOTA: Para obter mais informações sobre os componentes que podem ser instalados e em que locais para diferentes configurações, consulte o *Capítulo 1, Requisitos do Sistema*.

As opções a seguir estão disponíveis:

- Banco de Dados – instala o Banco de Dados do Sentinel.
- Servidor de Comunicação – instala o barramento de mensagens (iSCALE)
- Consultor
- Mecanismo de Correlação
- DAS
- Serviço do Coletor
- Sentinel Control Center
- Gerenciador de Dados do Sentinel
- HP OpenView Service Desk*
- Integração do Remedy*

NOTA: *Para obter informações sobre a instalação do HP OpenView Service Desk ou da Integração do Remedy, consulte o *Guia de Integração de Terceiros*.

NOTA: Se nenhum dos recursos filhos de "Serviços do Sentinel" for selecionado, anule a seleção do recurso *Serviços do Sentinel* também. Ele ficará esmaecido com uma marca de seleção se ainda estiver selecionado, mas todos os recursos filho serão desmarcados.

NOTA: Como parte da instalação do componente Banco de Dados de Sentinel, o instalador irá colocar arquivos na pasta $ESEC_HOME/utilities/db.

12. Se você selecionou a instalação do DAS, será solicitado a fornecer:
    - Número de Série
    - Chave de Licença
13. Se você selecionou a instalação de qualquer componente de integração de terceiros, será solicitado a fornecer uma senha para desbloquear o(s) componente(s) de integração de terceiros selecionados. Para obter mais informações, consulte o *Guia de Integração de Terceiros.*
14. Especifique o nome de usuário do Administrador do Sentinel no sistema operacional e o local do diretório pessoal. Esse é o nome de usuário que terá a propriedade do produto Sentinel instalado. Se o usuário não existir ainda, um usuário será criado com um diretório pessoal no diretório especificado.
    - Nome de usuário do Administrador do sistema operacional – O padrão é esecadm
    - Diretório pessoal do Administrador do sistema operacional – O padrão é "/export/home". Se o nome de usuário for esecadm, o diretório pessoal do usuário será /export/home/esecadm.

NOTA: Se um novo usuário for criado, sua senha precisará ser definida manualmente, separadamente desse instalador. Recomenda-se enfaticamente que isso seja feito diretamente pelo registro no sistema após a instalação do produto.

Para obedecer as rígidas configurações de segurança exigidas pela Certificação de Critérios Comuns, o Sentinel exige uma senha forte com as seguintes características:

1. Escolha senhas com no mínimo 8 caracteres, que incluam ao menos um dígito em MAIÚSCULA, um em minúscula, um símbolo especial (#$_) e um dígito numérico (0-9). Não use espaços.

2. A senha não pode conter o nome usado no e-mail nem partes do nome completo.

3. A senha não deve ser uma palavra "comum" (por exemplo, não deve ser uma palavra registrada em dicionário nem gíria de uso comum).

4. A senha não deve conter palavras de idioma algum, pois existem vários programas de invasão de senha capazes de verificar milhões de possibilidades de combinações de palavras em segundos.

5. Escolha uma senha de que possa se lembrar, mas que seja complexa. Por exemplo, Mft5#AIdade (Meu filho tem 5 anos de idade) OU EmnCh5#a (Eu moro na Califórnia há 5 anos).

15. Se optar por instalar o Sentinel Control Center, aparecerá um prompt de tamanho de heap JVM (Java Virtual Machine):
    - Tamanho de heap JVM (MB) - Por padrão, é definido como metade do tamanho da memória física detectada na máquina, com um máximo de 1024 MB. Esse será o tamanho de heap JVM máximo usado somente pelo Sentinel Control Center.

```
The installer has detected 2048 MB of physical memory. Please specify
the desired JVM heap size for Sentinel Control Center. The legal
range is 64-1024.

JVM Heap Size (MB)
1024
```

16. Se você optar por instalar o Serviço do Coletor, escolha proteger ou não proteger o Gerenciador do Coletor com uma senha. Se você optar por proteger o Gerenciador do Coletor, será solicitado a criar uma senha para ele.

NOTA: Para a proteção do Coletor com uma senha, será necessário digitar essa senha ao fazer o upload, download ou depuração de Coletores nesse Gerenciador do Coletor. Essa senha complementa o nome de usuário e senha do Sentinel necessários para fazer o login no Construtor de Coletor.

NOTA: Para obedecer as rígidas configurações de segurança exigidas pela Certificação de Critérios Comuns, o Sentinel exige uma senha forte com as seguintes características:

1. Escolha senhas com no mínimo 8 caracteres, que incluam ao menos um dígito em MAIÚSCULA, um em minúscula, um símbolo especial (!@#$%^&*()_+), e um dígito numérico (0-9).

2. A senha não pode conter o nome usado no e-mail nem partes do nome completo.

3. A senha não deve ser uma palavra "comum" (por exemplo, não deve ser uma palavra registrada em dicionário nem gíria de uso comum).

4. A senha não deve conter palavras de idioma algum, pois existem vários programas de invasão de senha capazes de verificar milhões de possibilidades de combinações de palavras em segundos.

5. Escolha uma senha de que possa se lembrar, mas que seja complexa. Por exemplo, Mft5#AIdade (Meu filho tem 5 anos de idade) OU EmnCh5#a (Eu moro na Califórnia há 5 anos).

17. Se optar por instalar o DAS, selecione a quantidade de RAM do sistema que deseja alocar para o Serviço de Acesso a Dados. No caso de ambientes distribuídos, recomenda-se selecionar o máximo de memória (4 GB). No caso de ambientes independentes, recomenda-se selecionar metade da memória RAM.

18. Para a instalação do banco de dados, será solicitado o seguinte:
    a. Selecione a plataforma do servidor do banco de dados de destino como Oracle 9i e selecione uma das ações a seguir:
        - Criar um novo banco de dados com objetos de banco de dados – cria uma nova instância de banco de dados Oracle e preenche a nova instância com objetos de banco de dados.

- Adicionar objetos de banco de dados a um banco de dados vazio existente – somente adiciona um banco de dados a uma instância de banco de dados Oracle existente. A instância de banco de dados Oracle existente precisa estar vazia, exceto pela presença do usuário esecdba.

b. Digite o diretório de registro de instalação do banco de dados (padrão: $ESEC_HOME/logs/db). Aceite o ‘Diretório do registro de instalação do banco de dados’ padrão ou clique em *Procurar* para especificar um local diferente.

Selecione a plataforma do servidor do banco de dados de destino:

Oracle 9i

Criar um novo banco de dados com objetos de banco de dados.

Adicionar objetos de banco de dados a um banco de dados vazio existente.

Diretório do registro de instalação do banco de dados:

/opt/sentinel5.1.3.0/logs/db

Procurar

c. Clique em *OK* no nome de usuário do Oracle padrão.

d. Se você optar por criar um novo banco de dados, digite o seguinte:

- O caminho para o arquivo de driver do Oracle JDBC (o nome típico do arquivo .jar é ojdbc14.jar). Esse é o caminho completo para o arquivo .jar, normalmente $ORACLE_HOME/jdbc/lib/ojdbc14.jar (não é possível usar variáveis de ambiente nesse campo).
- Nome de host – O nome de host da máquina onde o banco de dados será instalado. Esse campo não é configurável se uma nova instância de banco de dados estiver sendo criada.
- Nome do Banco de Dados – O nome da instância de banco de dados que será instalada.

e. Se você optou por adicionar objetos de bancos de dados a um banco Oracle vazio existente, será solicitado a fornecer as informações a seguir.

- O caminho para o arquivo de driver do Oracle JDBC (o nome típico do arquivo .jar é ojdbc14.jar). Esse é o caminho completo para o arquivo .jar, normalmente $ORACLE_HOME/jdbc/lib/ojdbc14.jar (não é possível usar variáveis de ambiente nesse campo).

- Nome de host do banco de dados ou endereço IP – O nome ou endereço IP do host onde está o banco de dados Oracle ao qual você deseja adicionar objetos de banco de dados. Pode ser o nome de host local ou um nome de host remoto.
- Nome do banco de dados – O nome da instância do banco de dados Oracle vazio existente à qual você deseja adicionar objetos de banco de dados (o padrão é ESEC). Esse nome de banco de dados precisa aparecer como nome de um serviço no arquivo tnsnames.ora (no diretório $ORACLE_HOME/network/admin/) da máquina onde o instalador está sendo executado.

NOTA: Se o nome do banco de dados não estiver no arquivo tnsnames.ora, o instalador não exibirá um erro nesse momento da instalação (porque ele verifica a conexão usando uma conexão JDBC direta), mas a instalação do Banco de dados irá falhar quando o instalador tentar se conectar ao banco de dados por meio de sqlplus. Se a instalação do Banco de dados falhar nesse ponto, você pode voltar até esse prompt e corrigir o nome do banco de dados.

- Porta do banco de dados (o padrão é 1521).
- Para o usuário Administrador do Banco de Dados do Sentinel (DBA), especifique a senha do usuário "esecdba". O campo de nome de usuário desse prompt não é editável.

f. Se você optou por criar um novo banco de dados, verá o prompt a seguir:

- Memória Oracle (MB) – A quantidade de memória RAM a ser alocada a essa instância de banco de dados Oracle.
- Porta de Escuta – a porta onde criar uma escuta Oracle (o padrão é 1521).
- Senha e confirmação de senha do usuário SYS – SYS é um usuário do Oracle padrão. A senha desse usuário será definida como o valor especificado aqui.
- Senha e confirmação de senha do usuário SYSTEM – SYSTEM é um usuário do Oracle padrão. A senha desse usuário será definida como o valor especificado aqui.

g. Se você optar por criar um novo banco de dados, será solicitado a digitar o tamanho do banco: Você tem as opções a seguir:
   - Padrão (20 GB)
   - Grande (400 GB)
   - Personalizado (especifique manualmente o tamanho). Se você escolher essa opção, será solicitado a fornecer:
   - o tamanho inicial de cada arquivo de banco de dados em MB (100 a 10.000)
   - o tamanho máximo de cada arquivo de banco de dados em MB (2.000 a 100.000)
   - o tamanho de todos os arquivos de banco de dados em MB (7.000 a 2.000.000)
   - o tamanho de cada arquivo de registro em MB (100 a 100.000)

h. Se você optar por criar um novo banco de dados, será solicitado a digitar o local de armazenamento dos arquivos de bancos de dados a seguir:

NOTA: Para fins de recuperação e desempenho, recomenda-se que esses locais estejam em dispositivos de E/S diferentes.

Como o instalador não irá criar esses diretórios, eles precisam ser criados externamente antes de avançar.

Esses diretórios precisam permitir gravação pelo usuário do Oracle.

   - Diretório de dados
   - Diretório de índices
   - Diretório de Dados de Resumo
   - Diretório de Índices de Resumo
   - Diretório Temporário e Desfazer Tabela:
   - Diretório A do Membro de Redo Log
   - Diretório B do Membro de Redo Log

Please enter the storage location for the following database files.

Data Directory:	/opt/oracle
Index Directory:	/opt/oracle
Summary Data Directory:	/opt/oracle
Summary Index Directory:	/opt/oracle
Temp and Undo Directory:	/opt/oracle
Redo Log Member A Directory:	/opt/oracle
Redo Log Member B Directory:	/opt/oracle

i. Se você optou por criar um novo banco de dados, digite as informações de autenticação do Administrador do Banco de Dados do Sentinel (DBA). Este é o esecdba, o proprietário dos objetos de banco de dados.

j. Digite as informações de autenticação do usuário do banco de dados do aplicativo Sentinel. Este é o esecapp, o nome do usuário do aplicativo Sentinel que os processos do Sentinel usam para a conexão com o banco de dados.

k. Digite as informações de autenticação do usuário do Banco de Dados do Administrador do Sentinel. Este é o esecadm, o usuário Administrador do Sentinel.

l. Clique em *Avançar* na janela de resumo da instalação do banco de dados.

19. Se você optou por instalar o DAS, mas não optou por instalar o Banco de Dados do Sentinel, será solicitado a fornecer as informações do Banco de dados do Sentinel para Oracle a seguir. Essas informações serão usadas para configurar o DAS para que aponte para o Banco de Dados do Sentinel.

    - Nome de host do banco de dados ou endereço IP – O nome ou endereço IP do Banco de Dados do Sentinel para Oracle a ser configurado para se conectar ao componente DAS.
    - Nome do banco de dados – O nome da instância de banco de dados Oracle vazia a ser configurada para se conectar ao componente DAS (o padrão é ESEC).
    - Porta do banco de dados (o padrão é 1521).
    - Para o Usuário do Banco de Dados do Aplicativo Sentinel, especifique o login "esecapp" e digite a senha dada para esse usuário durante a instalação do Banco de Dados do Sentinel.

20. Se você optou por instalar o DAS, configure o suporte de e-mail do Sentinel. Especifique o servidor SMTP e o endereço de e-mail do remetente a ser usado pelo Serviço de Execução para enviar mensagens (opcional – você pode editar isso manualmente após instalar [$ESEC_HOME\sentinel\config\execution.properties]):

SMTP Server:

"From" EmailAddress:

21. Se você optou por instalar o Advisor, selecione o tipo de instalação (se a opção Consultor foi escolhida, um nome de usuário e senha)
    - Download Direto da Internet – A máquina do Advisor está diretamente conectada à Internet. Nessa configuração, é feito o download automático das atualizações do Sentinel da Internet com regularidade.
    - Independente – O Advisor é configurado como um sistema isolado que requer intervenção manual para receber uma atualização do Sentinel.
22. Se você optou por instalar o Advisor e selecionou o uso do Download Direto da Internet, digite seu nome de usuário, senha e freqüência de atualização dos dados do Advisor. Se o nome de usuário ou senha não puder ser verificado, após clicar em *Avançar* você será perguntado se deseja continuar (não recomendado). Se optar por continuar, digite a senha do Advisor novamente na janela de confirmação de senha. Caso contrário, corrija a senha do Advisor.

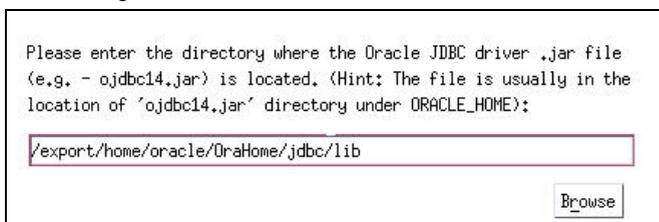
Please enter the username and password to access the Advisor server and feed data:

Username:

Password:

Please select how often Advisor data needs to be updated:

6 Hours   12 Hours

23. Se você optou por instalar o Advisor, digite o caminho até o diretório que contém o driver do Oracle JDBC (o nome típico do arquivo de driver é ojdbc14.jar). Esse é o caminho completo para o diretório que contém o arquivo .jar do driver, normalmente $ORACLE_HOME/jdbc/lib (não é possível usar variáveis de ambiente nesse campo).

Please enter the directory where the Oracle JDBC driver .jar file (e.g. - ojdbc14.jar) is located. (Hint: The file is usually in the location of 'ojdbc14.jar' directory under ORACLE_HOME):

/export/home/oracle/OraHome/jdbc/lib

Browse

24. Se você optou por instalar o Advisor, digite:
    - O diretório onde serão armazenados os arquivos de alimentação de dados do Advisor. Esse é o local onde serão gravados os arquivos de alimentação de ataque e alerta quando for feito seu download.

NOTA: Os arquivos de alimentação de dados do Advisor precisam ter as configurações de propriedade a seguir:

Usuário – esecadm

Grupo – esec

Se o diretório não tiver essas configurações de propriedade, execute o comando a seguir como usuário raiz para definir a propriedade do diretório:

```
chown esecadm:esec <caminho_do_diretório>
```

- Endereço do remetente, que será exibido nas notificações de e-mail
- Endereço do destinatário para o envio de notificações por e-mail

NOTA: Após a instalação, para mudar os endereços de e-mail do Advisor, edite os arquivos attackcontainer.xml e alertcontainer.xml no diretório $ESEC_HOME/sentinel/config. Para obter mais informações, consulte o *Capítulo 7 – Guia Consultor do Guia do Usuário do Sentinel*.

- Selecione Sim ou Não para o recebimento de e-mails sobre atualizações bem sucedidas do Advisor. As notificações de erro serão sempre enviadas.

25. Se você optou por instalar o HP Service Desk ou a Integração do Remedy, será solicitado a fornecer informações adicionais. Para obter mais informações, consulte o *Guia de Integração de Terceiros do Sentinel*.
26. Leia as informações apresentadas nas telas que aparecerem e clique em *Avançar* ao concluir. Depois de concluída a instalação, será necessário reinicializar. Clique em *Concluir* para reinicializar o sistema.
27. O instalador do Sentinel desliga o Registro de Arquivos por padrão. Para fins de recuperação de bancos de dados, é altamente recomendável que, após a instalação e antes de começar a receber dados de eventos de produção, você habilite o Registro de Arquivos. Você também deve programar um backup dos seus registros de arquivo para liberar espaço no destino do registro de arquivos, do contrário o banco de dados irá parar de aceitar eventos.

28. Se você espera uma taxa de eventos elevada (superior a 500 eventos por segundo), é necessário seguir as instruções de configuração adicionais contidas na seção Configurando a Estratégia de Inserção de Eventos da Interface de Chamada Oracle (OCI).

Pós-instalação do Sentinel 5 para Oracle

Atualizando o e-mail do Sentinel para autenticação SMTP

Se o sistema exigir autenticação SMTP, você precisará atualizar o arquivo execution.properties. Esse arquivo está na máquina em que o DAS foi instalado. Ele está localizado em $ESEC_HOME/sentinel/config. Para configurar esse arquivo, execute mailconfig.sh para mudar o arquivo e mailconfigtest.sh para testar as mudanças.

Para configurar o arquivo execution.properties

1. Na máquina em que o DAS foi instalado, faça login como esecadm e mude para o diretório:

```
$ESEC_HOME/sentinel/config
```

2. Execute mailconfig desta maneira:

```
./mailconfig.sh -host <servidor SMTP> -from <endereço
   de e-mail de origem> -user <usuário de autenticação
   de e-mail> –password
```

Exemplo:

```
./mailconfig.sh -host 10.0.1.14 -from
   meu_nome@domínio.com -user meu_nome_de_usuário
   –password
```

Depois de digitar esse comando, você será solicitado a fornecer uma nova senha.

```
Digite a senha:*********

Confirme a senha:*********
```

NOTA: Ao usar a opção password, ela deve ser o último argumento.

Para testar a configuração de execution.properties

1. Na máquina em que o DAS foi instalado, faça login como esecadm e mude para o diretório:

```
$ESEC_HOME/sentinel/config
```

2. Execute mailconfigtest desta maneira:

```
./mailconfigtest.sh -to <endereço de e-mail de destino>
```

Se o e-mail for enviado com êxito, será exibida a seguinte saída na tela e o e-mail será recebido no endereço de destino.

```
O e-mail foi enviado com êxito!
```

Verifique a caixa de correio do e-mail de destino para confirmar o recebimento da mensagem. A linha de assunto e o conteúdo devem ser:

```
Assunto: Testando a propriedade de e-mail do Sentinel

Este é um teste da configuração da propriedade de e-mail
   do Sentinel. Se você vir esta mensagem, a propriedade
   de e-mail do Sentinel foi configurada corretamente
   para enviar e-mail
```

Banco de Dados do Sentinel

Após instalar o Banco de Dados do Sentinel, o banco irá conter os usuários padrão a seguir:

- esecdba – Proprietário do esquema de bancos de dados. O privilégio de DBA não é concedido ao usuário esecdba por questões de segurança. Para usar o Enterprise Manager, crie um usuário com privilégios de DBA.
- esecapp – Usuário do aplicativo de banco de dados. Este é o usuário do aplicativo utilizado para a conexão com o banco de dados.
- esecadm – Usuário do banco de dados que é o Administrador do Sentinel. Não é a mesma conta do usuário do sistema operacional esecadm.
- esecrpt – Usuário do relatório de bancos de dados
- SYS – Usuário do banco de dados SYS
- SYSTEM – Usuário do banco de dados SYSTEM

Serviço do Coletor

Durante a instalação do Serviço do Coletor, os seguintes Coletores serão instalados, cada qual com uma configuração de porta para sua execução.

Produto	**Nome do Coletor**
Coletores Demo	
Teste de upload de bens, funciona com o Coletor DemoEvents	DemoAssetUpload
Teste de eventos demo, funciona com o Coletor DemoAssetUpload e com o DemoVulnerabilityUpload	DemoEvents
Teste de upload de vulnerabilidade, funciona com o Coletor DemoEvents	DemoVulnerabilityUpload
Teste de envio de um evento	SendOneEvent
Teste de envio de vários eventos	SendMultipleEvents

NOTA: Para obter mais informações sobre a configuração dos Coletores Demo, consulte o *Capítulo 12 - Teste da Instalação.*

NOTA: Para ver Coletores adicionais, vá até o Sentinel Customer Portal. Para obter mais informações (inclusive sobre configuração) consulte a documentação que acompanha cada Coletor em:

$WORKBENCH_HOME/Elements/<nome do Coletor>/Docs/

Para instalar Coletores adicionais, execute o script do Service Pack no CD do Service Pack.. O script irá instalar os Coletores em nível local.

No Windows:

```
.\service_pack.bat
```

No UNIX:

```
./service_pack.sh
```

Para obter as instruções de instalação do Service Pack e uma lista de Coletores, consulte as *notas do Service Pack Release*.

Atualizando a Chave de Licença

Como atualizar a chave de licença (Solaris)

1. Faça login como usuário esecadm.
2. Vá até $ESEC_HOME/utilities.
3. Digite o seguinte comando:

```
./softwarekey
```

4. Digite o número 1 como a chave principal. Pressione Enter.

Criando uma Instância Oracle para o Banco de Dados do Sentinel

NOTA: Esse procedimento é apresentado a título de exemplo caso você deseje criar tabelas próprias em comparação com o uso do recurso de criação de tabelas do CD de instalação. Os valores de tamanho podem variar dependendo da configuração e dos requisitos do sistema. Os nomes das tabelas devem seguir exatamente as especificações abaixo.

Na instância Oracle, será necessário configurar:

- parâmetros
- tabelas

Criando uma Instância Oracle

1. Faça login como usuário Oracle.
2. Use a interface gráfica do Assistente de Banco de Dados Oracle para criar o seguinte:

NOTA: Os valores podem variar dependendo da configuração e dos requisitos do sistema.

Parâmetros Mínimos Recomendados para Configuração do Solaris	
Parâmetros	**Tamanho (bytes ou outra especificação)**
db_cache_size	1 GB
java_pool_size	33,554,432
large_pool_size	8,388,608
shared_pool_size	100 MB

Parâmetros Mínimos Recomendados para Configuração do Solaris	
Parâmetros	**Tamanho (bytes ou outra especificação)**
pga_aggregate_target	150,994,944
sort_area_size	109,051,904
open_cursors	500
cursor_sharing	SIMILAR
hash_join_enabled	TRUE
optimizer_index_caching	50
optimizer_index_cost_adj	55

Tamanho Mínimo Recomendado para Tabela do Solaris		
Tabela	**Tamanho de Exemplo**	**Notas**
REDO	3 x 100M	Este é o valor mínimo. Você deve criar redo logs maiores se tiver um EPS elevado.
SYSTEM	500M	Valor mínimo
TEMP	1G	Valor mínimo
UNDO	1G	Valor mínimo
ESENTD	5G	Valor mínimo Este é para dados de eventos
ESENTD2	500M	Valor mínimo Dados de configuração, bens, vulnerabilidade e associações (autoextend habilitado)
ESENTWFD	250M	Para dados do iTrac (autoextend habilitado)
ESENTWFX	250M	Para índice do iTrac (autoextend habilitado)
ESENTX	3G	Valor mínimo Para índice de eventos
ESENTX2	500M	Valor mínimo Índice de configuração, bens, vulnerabilidade e associações (autoextend habilitado)
SENT_ADVISORD	200M	Valor mínimo Para dados do Advisor (autoextend habilitado)
SENT_ADVISORX	100M	Valor mínimo Para índice do Advisor (autoextend habilitado)
SENT_LOBS	100M	Valor mínimo Para objetos grandes de bancos de dados (autoextend habilitado)
SENT_SMRYD	3G	Valor mínimo Para dados de resumo de Agregação
SENT_SMRYX	2G	Valor mínimo Para índice de resumo de Agregação

3. Execute o script createEsecdba.sh encontrado no diretório sentinel\dbsetup\bin no CD de Instalação do Sentinel. Este script irá criar o usuário esecdba, que é necessário para adicionar objetos de bancos de dados com o uso do instalador do Sentinel.
4. Faça um backup do banco de dados.

Configurando a Estratégia de Inserção de Eventos da Interface de Chamada Oracle (OCI)

O Sentinel 5.1 oferece uma estrutura para a inclusão de diferentes estratégias para a inserção de eventos no banco de dados. O Sentinel 5.1 oferece duas estratégias para a inserção de eventos no banco de dados Oracle.

- JDBCLoadStrategy
- OCILoadStrategy

A estratégia a ser usada para a inserção de eventos é regida pela propriedade da estratégia de inserção do componente EventStoreService do arquivo das_binary.xml.

A estratégia JDBC é a estratégia padrão configurada out of the box.

A estratégia OCI é uma estratégia de inserção nativa para a agilização da inserção de eventos. Essa estratégia requer que as bibliotecas OCI do Oracle estejam instaladas na máquina que está executando o componente DAS. A estratégia OCI precisa ser usada em configurações para as quais é esperada uma alta taxa de eventos.

O número de eventos a ser agrupado para inserção no banco de dados é regido pela propriedade insert.batchsize. Essa propriedade insert.batchsize é usada por todas as estratégias de inserção de eventos.

Para mudar a estratégia de inserção de eventos do Sentinel da Estratégia de Inserção JDBC padrão para a Estratégia de Inserção OCI, há algumas etapas que precisam ser executadas.

Mudando a estratégia de inserção de eventos da Estratégia JDBC para a OCI.

1. Verifique se as bibliotecas OCI do Oracle estão instaladas na máquina que está executando o componente DAS do Sentinel. Você precisará saber o caminho para o ORACLE_HOME nas etapas a seguir.
2. Faça login na máquina partindo da etapa 1 como o usuário esecadm.
3. Crie um arquivo ".profile" no diretório pessoal do usuário esecadm. Coloque o texto a seguir nesse arquivo (modifique o caminho para o ORACLE_HOME para que corresponda à sua instalação):

```
ORACLE_HOME=/build/home/oracle/OraHome
export ORACLE_HOME
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$ORACLE_HOME/lib
export LD_LIBRARY_PATH
```

4. Abra o arquivo $ESEC_HOME/sentinel/config/das_binary.xml para editá-lo em qualquer editor de texto.
5. Faça uma pesquisa no texto a seguir:

```
JDBCLoadStrategy
```

6. Mude esse texto para:

```
OCILoadStrategy
```

7. Grave esse mudança no arquivo das_binary.xml.

8. Reinicie o aplicativo binário DAS. (É fácil reiniciar o Binário DAS realizando um "ps –ef | grep DAS_Binary" para obter o ID do processo, eliminando esse processo e em seguida permitindo que o Watchdog do Sentinel automaticamente reinicie o processo.)

   Após o reinício do Binário DAS, a biblioteca $ESEC_HOME/sentinel/lib/libocievent.so será carregada e usada para realizar as inserções de Eventos no banco de dados via OCI.

Opções adicionais de Inserção de Eventos OCI

Além de especificar a "OCILoadStrategy" no arquivo das_binary.xml, há várias outras opções relacionadas a OCI que também podem ser configuradas.

- insert.batchsize – Essa definição permite configurar o máximo número de Eventos para inserção no banco de dados de uma só vez.
- insert.oci.workerCount – Essa definição permite configurar o número de threads usadas para inserir dados de Eventos no banco de dados.
- insert.oci.queueWaitTime – Essa configuração especifica o tempo máximo, em segundos, para aguardar antes de inserir os dados da fila de entrada no banco de dados. Sempre que um "tamanho de lote" de eventos é recebido, o lote inteiro é inserido. Mas o fluxo de entrada de eventos é lento, o tempo de espera da fila é usado para determinar o momento da inserção no banco de dados (mesmo que um lote completo de eventos ainda não tenha sido recebido).
- insert.oci.highWatermark – A alta marca d'água da fila do Evento de entrada.
- insert.oci.lowWatermark – A marca d'água baixa da fila do Evento de entrada.
- insert.oci.optimizationFlag – Flag de otimização. "ligada" ou "desligada".

Dicas de Depuração de OCI

A interface OCI irá registrar mensagens no arquivo $ESEC_HOME/sentinel/log/ocievent.log. As mensagens iniciais gravadas no arquivo de registro devem incluir mensagens de conexão de banco de dados bem sucedidas (ou fracassadas)… Este é um bom local para verificar se a biblioteca OCI foi carregada e configurada corretamente.

A interface OCI também irá registrar erros no arquivo das_binary localizado no diretório $ESEC_HOME/sentinel/log. Os erros registrados no arquivo de registro das_binary log incluem falhas na localização/carregamento da biblioteca libocievent.so, falhas de conexão ao banco de dados e falhas de inserção de Associações de Eventos/Evento.

Se houver mensagens de erro indicando que o arquivo "libocievent.so" não está sendo localizado ou carregado, então há três coisas a serem verificadas:

1. Verifique se as bibliotecas OCI Oracle estão instaladas.
2. Verifique se o arquivo "libocievent.so" está localizado no diretório $ESEC_HOME/sentinel/lib.
3. Verifique se o diretório $ESEC_HOME/sentinel/lib está no caminho "LD_LIBRARY_PATH" do usuário "esecadm". Em caso negativo, você pode atualizar o caminho LD_LIBRARY_PATH no perfil do usuário "esecadm".
4. Verifique se as variáveis de ambiente ORACLE_HOME e LD_LIBRARY_PATH estão atualizadas corretamente nas variáveis de ambiente do usuário esecadm conforme descrito na seção "Mudando a estratégia de inserção de eventos da Estratégia JDBC para a OCI".

4 Instalando o Sentinel 5 para Oracle no Linux

NOTA: O termo Agente é sinônimo de Coletor. De agora em diante, Agentes serão referidos como Coletores.

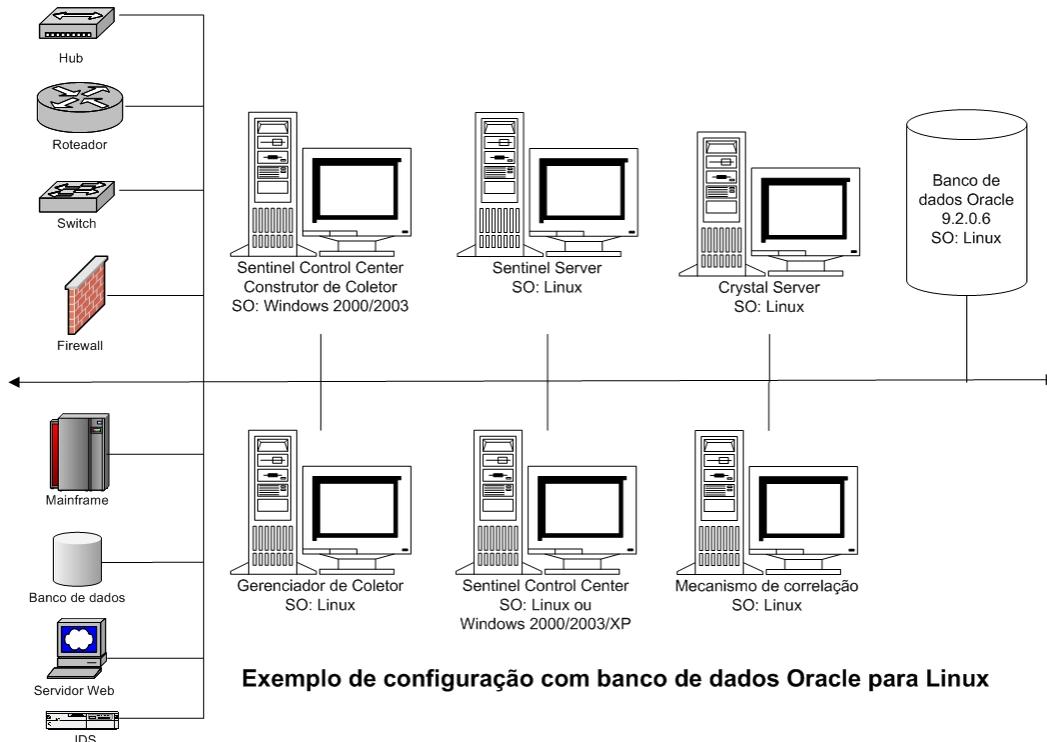
Este capítulo descreve a instalação do Sentinel Enterprise Security Management Sentinel 5 para Oracle no SuSE Linux Enterprise Server e Red Hat Enterprise Linux.

Pré-instalação do Sentinel 5 para Oracle no Linux

NOTA: Antes da instalação, assegure-se de que as máquinas atendem aos requisitos mínimos do sistema e que o sistema operacional foi "reforçado" com o uso das melhores práticas de segurança atuais.

NOTA: Instale o Oracle Enterprise com particionamento. O Gerenciador de Dados do Sentinel precisa desse recurso para gerenciar o Banco de dados do Sentinel.

NOTA: Ao realizar uma instalação limpa do Sentinel depois de ter uma versão anterior do Sentinel instalada, é necessário remover alguns arquivos e configurações do sistema que podem ter sobrado de uma instalação anterior. Se esses arquivos ou configurações não forem removidos, uma nova instalação limpa pode falhar. Esse procedimento deve ser realizado em cada máquina onde esteja sendo feita uma instalação limpa. Para obter mais informações, veja o *Apêndice E*.

A seguir estão configurações típicas do Linux para Sentinel. A configuração pode ser diferente dependendo do ambiente. Independentemente da configuração escolhida, é necessário instalar o banco de dados primeiro.

NOTA: Para obter mais informações sobre os sistemas operacionais suportados, consulte o *Capítulo 1 – Introdução, Plataformas Suportadas para o Sentinel Server no Linux*.

Obtendo uma Chave de Licença

O Serviço de Banco de Dados (DAS) do Sentinel Server requer uma chave de licença válida para instalar e executar o serviço. Essa chave de licença fica bloqueada na máquina onde o DAS será instalado. Uma chave de licença emitida para uma máquina não funciona em outra máquina.

Para obter a chave de licença, é necessário determinar o número de ID do host e fornecer essas informações para a Novell, que atribuirá uma chave de licença.

Para determinar a ID de host (Linux)

1. Faça login como usuário Root.
2. Insira e monte o CD de instalação do Sentinel.
3. use o comando cd para mudar para utilitários/linux e digite:

```
./esechostid
```

4. Envie esse número de ID do host para o Suporte Técnico da Novell. Eles fornecerão a você uma chave de licença.

Banco de Dados do Sentinel

Antes de instalar o Banco de Dados do Sentinel, será necessário o seguinte:

- Para saber quais são os requisitos de hardware, consulte os *Capítulos 1 e 2*.
- SuSE Linux Enterprise Server 9 com SP2 ou Atualização 5 ES (x86) do Red Hat Enterprise Linux 3
- Oracle 9i Enterprise Edition 9.2.0.6 (SuSE Linux somente) ou 9.2.0.7 com particionamento
- Usuário do sistema operacional Oracle (padrão: Oracle)
- Verifique se as seguintes variáveis de ambiente estão definidas para o usuário do sistema operacional Oracle:

  ```
  ORACLE_HOME
  ORACLE_BASE
  PATH (é preciso ter $ORACLE_HOME/bin)
  ```

  - Embora não seja recomendado, se você criar manualmente a instância de banco de dados Oracle, consulte Criando uma Instância Oracle para o Banco de Dados Sentinel para ver instruções sobre a criação da instância Oracle. Caso você escolha essa opção, ainda será necessário usar o instalador para adicionar os objetos do banco de dados à instância de banco de dados Oracle recém criada (consulte Instalação Personalizada).

NOTA: Caso esteja usando uma instância de banco de dados Oracle existente ou criada manualmente, ela precisa estar vazia, exceto pela presença do usuário esecdba. A seção Criando uma Instância Oracle para o Banco de Dados do Sentinel contém instruções para a criação desse usuário caso ele ainda não exista.

- Se estiver usando o instalador para criar a instância de banco de dados Oracle (recomendável), serão necessários os caminhos de diretório para colocar os arquivos de banco de dados. Esses diretórios precisam já existir antes da execução do instalador já que ele não cria esses diretórios. Esses diretórios também precisam permitir gravação pelo usuário do sistema operacional Oracle (p. ex. – oracle).

NOTA: Por motivos de desempenho, dependendo de se tratar da instalação em RAID, e se o ambiente RAID permitir, o Redo Log deve apontar para o disco de gravação mais rápido que estiver disponível.

NOTA: Por padrão, o instalador define que as seguintes tabelas NÃO devem crescer automaticamente: ESENTD, ESENTX, SENT_SMRYD e SENT_SMRYX. Fica definido o crescimento automático de todas as outras tabelas. O motivo para não permitir o crescimento automático das tabelas ESENTD, ESENTX, SENT_SMRYD e SENT_SMRYX é que elas contêm dados de eventos e dados resumidos de eventos. A utilização do espaço para eventos e resumos pode ser altamente dinâmica. Essas tabelas devem ser monitoradas e estendidas de forma controlada, com base na configuração do sistema de arquivos e levando em consideração o equilíbrio de E/S e o backup e recuperação de bancos de dados.

O gerenciamento de partições SDM (arquivamento, descarte e adição de partições) deve ser programado de modo a manter os dados do evento dentro de um tamanho controlado.

Sentinel Server

NOTA: Se o Banco de Dados do Sentinel não for instalado ao mesmo tempo em que o Sentinel Server, será necessário instalar o Banco de Dados do Sentinel primeiro.

Antes de instalar o Sentinel Server, será necessário:

- Para saber quais são os requisitos de hardware, consulte os *Capítulos 1 e 2*.
- SuSE Linux Enterprise Server 9 com SP2 ou Atualização 5 ES (x86) do Red Hat Enterprise Linux 3
- Número de série e Chave de licença do Sentinel 5 (Para DAS). Para obter mais informações, consulte Obtendo uma Chave de Licença.
- Servidor SMTP – Necessário para o envio de e-mails do Sentinel.

Sentinel Control Center e Assistente

Antes de instalar o Sentinel Server, será necessário:

- Para obter os requisitos de hardware, consulte os *Capítulos 1 e 2*
- SuSE Linux Enterprise Server 9 com SP2 ou Atualização 5 ES (x86) do Red Hat Enterprise Linux 3 ou
- (Construtor de Coletor e Sentinel Control Center) – Windows 2000 ou 2003

Consultor

Para instalar o Advisor, será necessário obter um ID e senha do Advisor com o Sentinel. O Download Direto da Internet usa a porta 443.

NOTA: Caso pretenda usar o Advisor para o Exploit Detection somente, não é necessário instalar o software Crystal Enterprise. Isso só é obrigatório se a intenção for executar Crystal Reports para Sentinel. Consulte o Capítulo 10, Configuração do Consultor, para obter mais informações.

Pré-instalação do Oracle no Linux

Para a instalação do Oracle no Linux para Sentinel, as seguintes ações são necessárias:

- Definição de valores de kernel
- Criação de uma conta de grupo e de usuário do Oracle
- Definição de variáveis de ambiente para o usuário do Oracle
- Vinculação do gcc
- Aplicação do patch do sistema operacional do Linux para a Instalação do Oracle 9.2.0.4 (obtenha o patch p3006854_9204_LINUX diretamente da Oracle)
- Instalação do Oracle 9.2.0.4 (obtenha esse software diretamente da Oracle)
- Aplicação do patch do Oracle 9.2.0.4 no Oracle 9.2.0.6 (SuSE Linux somente) ou 9.2.0.7 (obtenha o patch para o Oracle 9.2.0.6 ou 9.2.0.7 diretamente da Oracle)

Definindo os valores de Kernel para Oracle no Linux (SuSE e Red Hat)

Para a instalação do Oracle no Linux, os seguintes valores de kernel têm de ser definidos.

ISENÇÃO DE RESPONSABILIDADE: A seguir estão sugestões de valores mínimos. Se as configurações do sistema excederem esses valores, não as altere. Consulte o administrador do sistema e a documentação do Oracle para obter mais informações.

- shmmax=2147483648 (valor mínimo)
- shmmni=4096
- semmns=32000
- semmni=1024
- semmsl=1024
- semopm=100

1. Efetue login como Usuário Root.
2. Para definir os parâmetros de kernel, adicione o texto a seguir ao final do arquivo "/etc/sysctl.conf":

NOTA: As configurações abaixo são os valores mínimos sugeridos. Se as configurações excederem esses valores, não as altere. Para determinar a configuração atual de um determinado parâmetro de kernel, execute o comando:

```
sysctl <kernel_parameter>
```

Por exemplo, para verificar o atual valor do parâmetro de kernel "kernel.sem", execute o comando:

```
sysctl kernel.sem
```

```
# Configurações de Kernel para o Oracle
# kernel.sem = <SEMMSL> <SEMMNS> <SEMOPM> <SEMMNI>
kernel.sem = 1024        32000   100      1024
kernel.shmmax = 2147483648
kernel.shmmni = 4096
fs.file-max = 65536
net.ipv4.ip_local_port_range = 1024 65000
```

3. Execute o comando a seguir para carregar as modificações no arquivo "/etc/sysctl.conf":

```
sysctl -p
```

4. Para definir os handles de arquivo e limites de processo, adicione o texto a seguir ao final do arquivo "/etc/security/limits.conf". "nproc" é o limite máximo do número de processos, e "nofile" é o limite máximo do número de arquivos abertos. Trata-se de valores recomendados, mas que podem ser modificados se necessário. O texto a seguir supõe que seu ID de usuário do Oracle é "oracle". Se o seu ID de usuário for diferente, substitua "oracle" no texto a seguir pelo seu ID de usuário do Oracle.

```
# Configurações adicionadas ao Oracle
oracle          soft    nproc   16384
oracle          hard    nproc   16384
oracle          soft    nofile  65536
oracle          hard    nofile  65536
```

Pré-instalação do Oracle no SuSE Linux

Pré-instalação do Oracle no SuSE Linux

ISENÇÃO DE RESPONSABILIDADE: As instruções a seguir não têm por objetivo substituir a documentação do Oracle. Trata-se apenas de um exemplo de cenário de configuração. Recomenda-se enfaticamente que essas instruções sejam seguidas. A configuração exata pode variar. Consulte a documentação do sistema operacional e do Oracle para obter mais informações.

1. Siga as instruções de instalação fornecidas no manual de instalação do SLES 9. Instale o SLES 9 com pacotes padrões junto com *Ferramentas e Compilador C/C++*.

   NOTA: Se você já instalou o SuSE Linux, você pode usar o YaST (Yet Another Setup Tool) no SuSE Linux para instalar *Ferramentas e Compilador C/C++*.

2. Efetue login como Usuário Root.
3. Verifique o nível de kernel digitando:

   ```
   uname –r
   ```

   Um valor de kernel de 2.6* é requerido. Por exemplo, um nível de kernel de 2.6.5-7.97 está OK.

4. Instale gcc_old-2.95.3-175.2.i586.rpm incluído no SLES 9 SP2 CD1.

   ```
   rpm -i <path>/ gcc_old-2.95.3-175.2.i586.rpm
   ```

5. Verifique se está executando o SP2 digitando:

   ```
   SPident
   ```

   ou

   ```
   cat /etc/SuSE-release
   ```

   Deve aparecer:

   ```
   CONCLUSÃO: O sistema está atualizado!
      Encontrado     SLES-9-i386-SP2
   ```

   ou

   ```
   SUSE LINUX Enterprise Server (i586)
   VERSION = 9
   PATCHLEVEL = 2
   ```

6. Para automatizar a maioria das tarefas de pré-instalação do Oracle e criar o usuário oracle, instale orarun-1.8-109.15.i586.rpm.

   NOTA: Consulte o documento de instalação do Oracle para obter uma lista completa dos pré-requisitos.

   ```
   rpm -i <path>/orarun-1.8-109.15.i586.rpm
   ```

   NOTA: orarun também está disponível em http://www.novell.com.orarun também irá:

   ```
   exportar LD_ASSUME_KERNEL=2.4.21
   exportar LD_PRELOAD=/usr/lib/libInternalSymbols.so
   ```

7. A conta para o usuário oracle está desativada. Ative-a alterando o shell para o usuário oracle de /bin/false para /bin/bash usando a administração de usuário do YaST ou editando o /etc/passwd.
8. Defina uma nova senha para o usuário oracle usando o YaST ou digitando:

   ```
   /usr/bin/passwd oracle
   ```

9. Para definir os parâmetros de kernel, execute

   ```
   /usr/sbin/rcoracle start
   ```

   Ignore qualquer erro.
10. Para instalar o Oracle 9.2.0.4, de dentro do Disk1, execute o script:

    ```
    ./runinstaller
    ```

11. Ao avançar no instalador, deixe todos os prompts em seus valores padrão, salvo se houver especificação em contrário abaixo.
    - Ao ser solicitado a fornecer o Nome do Grupo UNIX, digite: dba
    - Ao ser solicitado a fornecer o Tipo de Instalação, escolha Personalizada.

    Selecione os componentes a seguir para serem instalados:
    - Oracle 9i 9.2.0.4.0
    - Opções do Enterprise Edition 9.2.0.1.0
      - Particionamento do Oracle 9i 9.2.0.4.0
    - Serviços de rede do Oracle 9.2.0.1.0
      - Escuta de rede do Oracle 9.2.0.4.0
    - Produtos do Oracle Enterprise Manager 9.2.0.1.0 (Todos)
    - Oracle 9i Development Kit 9.2.0.1.0 (Todos)
    - Oracle 9i para Documentação do UNIX 9.2.0.1.0
    - Servidor HTTP do Oracle 9.2.0.1.0 (Todos)
    - iSQL*Plus 9.2.0.4.0 (Todos)
    - Interfaces do Oracle JDBC/OCI 9.2.0.1.0
12. Na solicitação para criar banco de dados, escolha NÃO.
13. Opcional, cancele todos os assistentes de configuração que o instalador iniciar.
14. Modifique o arquivo '/opt/oracle/network/admin/sqlnet.ora' (ou crie o arquivo se ele não existir) para que contenha o seguinte (remova qualquer informação sem comentário existente no arquivo):

    ```
    NAMES.DIRECTORY_PATH = (TNSNAMES, HOSTNAME)
    ```

15. Para aplicar o patch do Oracle 9.2.0.6 ao Instalador do Oracle, de dentro do Disk1 da distribuição de patch do Oracle 9.2.0.6, execute o script:

    NOTA: O patch do Oracle 9.2.0.6 NÃO será aplicado, a menos que primeiro seja aplicado um patch ao Instalador do Oracle.

    ```
    ./runInstaller
    ```

16. Ao avançar no instalador, deixe todos os prompts em seus valores padrão, salvo se houver especificação em contrário abaixo.
    - Na tela de boas-vindas, clique em *Avançar*.
    - Na tela Especificar Locais de Arquivos, escolha *OUIHome* como Nome de Destino na lista suspensa (ou o que você usar como Nome de Destino durante a instalação do Oracle 9.2.0.4). Clique em *Avançar*.
    - Na tela Selecionar Produto para Instalar, escolha *Instalador Universal do Oracle 10.1.0.3.0*. Clique em *Avançar*.
    - Na tela Resumo, revise o resumo de instalação e clique em *Instalar*.
    - Na tela Fim da Instalação, clique em *Sair*.
17. Para aplicar o patch do Oracle 9.2.0.6 ao Oracle, de dentro do Disk1 da distribuição de patch do Oracle 9.2.0.6, execute o script:

    ```
    ./runInstaller
    ```

18. Ao avançar no instalador, deixe todos os prompts em seus valores padrão, salvo se houver especificação em contrário abaixo.
    - Na tela de boas-vindas, clique em *Avançar*.
    - Na tela Especificar Locais de Arquivos, escolha "OUIHome" como Nome de Destino na lista suspensa (ou o que você usar como Nome de Destino durante a instalação do Oracle 9.2.0.4). Clique em *Avançar*.
    - Dependendo da versão, na tela Selecionar Produto para Instalar, escolha *Oracle 9iR2 Patchset 9.2.0.6.0.* Depois, clique em *Avançar*.
    - Na tela Resumo, revise o resumo de instalação e clique em *Instalar*.
    - Na tela Fim da Instalação, clique em *Sair*.

Pré-instalação do Oracle no Red Hat Linux

Pré-instalação do Oracle no Red Hat Linux

ISENÇÃO DE RESPONSABILIDADE: As instruções a seguir não têm por objetivo substituir a documentação do Oracle. Trata-se apenas de um exemplo de cenário de configuração. Esta documentação supõe que o diretório pessoal dos usuários do Oracle é **/export/home/oracle** e que o Oracle será instalado em **/opt/oracle**. A configuração exata pode variar. Consulte a documentação do sistema operacional e do Oracle para obter mais informações.

1. Efetue login como Usuário Root.
2. Crie um grupo UNIX e uma conta de usuário UNIX para o proprietário do banco de dados Oracle.

   Adicione um grupo dba (como root):

   ```
   groupadd dba
   ```

3. Adicione o usuário do Oracle (como root):

   ```
   useradd –g dba –s /bin/bash –d /export/home/oracle –m
     oracle
   ```

4. Crie um diretório para ORACLE_HOME e ORACLE_BASE:

```
mkdir –p /opt/oracle/
```

5. Mude a propriedade do diretório ORACLE_BASE e complete para o oracle/dba:

```
chown -R oracle:dba /opt/oracle
```

6. Mude o usuário do Oracle:

```
su - oracle
```

7. Abra o arquivo '.bash_profile' (no diretório pessoal do usuário do Oracle) para editá-lo e adicione o seguinte ao final do arquivo:

NOTA: Esse conjunto de variáveis de ambiente somente devem ser usadas para o usuário do Oracle. Em termos específicos, elas não devem ser definidas no ambiente do sistema nem no ambiente do usuário esecadm.

```
# Defina a variável de ambiente LD_ASSUME_KERNEL somente
   para o Red Hat 9,
# RHEL AS 3 e RHEL AS 4 !!
# Use a implementação "Linuxthreads com coleções
   flutuantes" em vez de NPTL:
# para RH 9 e RHEL AS 3
exportar LD_ASSUME_KERNEL=2.4.1
# para RHEL AS 4
# exportar LD_ASSUME_KERNEL=2.4.19
# Ambiente Oracle
export ORACLE_BASE=/opt/oracle
export ORACLE_HOME=$ORACLE_BASE/
export ORACLE_SID=test
export ORACLE_TERM=xterm
# exportar TNS_ADMIN= Definir se sqlnet.ora,
   tnsnames.ora, etc. não estiverem em
   $ORACLE_HOME/network/admin
export NLS_LANG=AMERICAN;
export ORA_NLS33=$ORACLE_HOME/ocommon/nls/admin/data
LD_LIBRARY_PATH=$ORACLE_HOME/lib:/lib:/usr/lib
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/usr/local/lib
export LD_LIBRARY_PATH
# Definir caminhos de pesquisa de shell
export PATH=$PATH:$ORACLE_HOME/bin
```

8. Repita o login como usuário do Oracle para carregar mudanças de variáveis de ambiente a partir da última etapa:

```
sair
su - oracle
```

9. Vincule o gcc com a versão 2.9.6

NOTA: Se /usr/bin/gcc296 ou /usr/bin/g++296 não existir, gcc ou g++ não foi instalado. Nesse caso, instale esses componentes e retorne para essa etapa.

```
su - root
ln -s /usr/bin/gcc296 /usr/bin/gcc
ln -s /usr/bin/g++296 /usr/bin/g++
```

10. Saia para retornar ao prompt de usuário do Oracle.

```
sair
```

11. Execute o patch p3006854_9204_LINUX.zip do Oracle, que aplica o patch do sistema operacional Linux para a instalação do Oracle. Esse patch pode ser obtido com a Oracle.

```
su - root
descompacte p3006854_9204_LINUX.zip
cd 3006854
sh rhel3_pre_install.sh
```

12. Saia para retornar ao prompt de usuário do Oracle.

```
sair
```

13. Para instalar o Oracle 9.2.0.4, de dentro do Disk1, execute o script:

```
./runInstaller
```

14. Ao avançar no instalador, deixe todos os prompts em seus valores padrão, salvo se houver especificação em contrário abaixo.
    - Ao ser solicitado a fornecer o Nome do Grupo UNIX, digite: dba
    - Ao ser solicitado a fornecer o Tipo de Instalação, escolha Personalizada.

    Selecione os componentes a seguir para serem instalados:
    - Oracle 9i 9.2.0.4.0
    - Opções do Enterprise Edition 9.2.0.1.0
        - Particionamento do Oracle 9i 9.2.0.4.0
    - Serviços de rede do Oracle 9.2.0.1.0
        - Escuta de rede do Oracle 9.2.0.4.0
    - Produtos do Oracle Enterprise Manager 9.2.0.1.0 (Todos)
    - Oracle 9i Development Kit 9.2.0.1.0 (Todos)
    - Oracle 9i para Documentação do UNIX 9.2.0.1.0
    - Servidor HTTP do Oracle 9.2.0.1.0 (Todos)

- iSQL*Plus 9.2.0.4.0 (Todos)
- Interfaces do Oracle JDBC/OCI 9.2.0.1.0

15. Ao ser solicitado a criar banco de dados, escolha NÃO.
16. Opcional, cancele todos os assistentes de configuração que o instalador iniciar
17. Modifique o arquivo '/opt/oracle/network/admin/sqlnet.ora' (ou crie o arquivo se ele não existir) para que contenha o seguinte (remova qualquer informação sem comentário existente no arquivo):

    ```
    NAMES.DIRECTORY_PATH = (TNSNAMES, HOSTNAME)
    ```

18. Para aplicar o patch do Oracle 9.2.0.6 ou 9.2.0.7 ao Instalador do Oracle, de dentro do Disk1 da distribuição de patch do Oracle 9.2.0.6 ou 9.2.0.7, execute o script:

    NOTA: O patch do Oracle 9.2.0.6 NÃO será aplicado, a menos que primeiro seja aplicado um patch ao Instalador do Oracle.

    ```
    ./runInstaller
    ```

19. Ao avançar no instalador, deixe todos os prompts em seus valores padrão, salvo se houver especificação em contrário abaixo.
    - Na tela de boas-vindas, clique em *Avançar*.
    - Na tela Especificar Locais de Arquivos, escolha *OUIHome* como Nome de Destino na lista suspensa (ou o que você usar como Nome de Destino durante a instalação do Oracle 9.2.0.4). Clique em *Avançar*.
    - Na tela Selecionar Produto para Instalar, escolha *Instalador Universal do Oracle 10.1.0.3.0*. Clique em *Avançar*.
    - Na tela Resumo, revise o resumo de instalação e clique em *Instalar*.
    - Na tela Fim da Instalação, clique em *Sair*.
20. Para aplicar o patch do Oracle 9.2.0.6 ou 9.2.0.7 ao Oracle, de dentro do Disk1 da distribuição de patch do Oracle 9.2.0.6 ou 9.2.0.7, execute o script:

    ```
    ./runInstaller
    ```

21. Ao avançar no instalador, deixe todos os prompts em seus valores padrão, salvo se houver especificação em contrário abaixo.
    - Na tela de boas-vindas, clique em *Avançar*.
    - Na tela Especificar Locais de Arquivos, escolha "OUIHome" como Nome de Destino na lista suspensa (ou o que você usar como Nome de Destino durante a instalação do Oracle 9.2.0.4). Clique em *Avançar*.
    - Dependendo da versão, na tela Selecionar Produto para Instalar, escolha *Oracle 9iR2 Patchset 9.2.0.6.0* ou *Oracle 9iR2 Patchset 9.2.0.7.0*. Clique em *Avançar*.
    - Na tela Resumo, revise o resumo de instalação e clique em *Instalar*.
    - Na tela Fim da Instalação, clique em *Sair*.

22. Desvincule o gcc:

```
su – root
rm /usr/bin/gcc
rm /usr/bin/g++
```

23. Saia para retornar ao prompt de usuário do Oracle.

```
sair
```

Instalação do Sentinel 5 para Oracle no Linux

O Sentinel 5 dá suporte a dois tipos de instalação. São elas:

- Simples – Opção de instalação da all-in-one. Serviços do Sentinel, Serviço do Coletor e Aplicativos do Oracle na mesma máquina. O tipo de instalação se destina a fins demonstrativos apenas.
- Personalizado – Permite uma instalação totalmente distribuída.

Instalação Simples no Linux

Essa opção instala os componentes mais comuns (não inclui o Construtor de Coletor nem recursos de Integração de Terceiros) em uma única máquina. Se destina principalmente a fins demonstrativos. Não é recomendada para uso em um ambiente de teste ou produção.

NOTA: A instalação simples não oferece suporte à autenticação de senha do Gerenciador de Coletor.

Como realizar uma Instalação Simples

1. Verifique se você coletou as informações, realizou as tarefas e atendeu aos requisitos especificados na seção Pré-instalação do Sentinel 5 para Oracle em relação aos componentes que está instalando.
2. Verifique a configuração do Oracle no Linux.
3. Faça login como usuário Root.
4. Insira e monte o CD de instalação do Sentinel.
5. Para iniciar o programa de instalação, vá para o diretório de instalação no CD-ROM e digite:

   Para o modo de interface gráfica:

   ```
   ./setup.sh
   ```

   ou

   Para modo textual:

   ```
   ./setup.sh –console
   ```

6. Clique na seta para baixo e selecione uma das seguintes opções de idioma:
   - Inglês.
   - Francês
   - Alemão
   - Italiano
   - Português
   - Espanhol
7. Siga os prompts do instalador.
8. Depois de ler a tela de boas-vindas, clique em *Avançar*.

9. Aceite o Contrato de Licença de Usuário Final e clique em *Avançar*.
10. Aceite o diretório de instalação padrão ou clique em *Procurar* para especificar o local da instalação. Clique em *Avançar*.

Nome do directório:
/opt/sentinel5.1.3.0
Procurar

11. Selecione *Simples*. Clique em *Avançar*.

12. Digite as informações sobre a configuração.
    - Número de Série e Chave de Licença
    - Servidor SMTP (o nome DNS ou o endereço IP) – essa opção permite ao Sentinel enviar e-mails.
    - Email – digite um endereço de e-mail válido para o qual os e-mails de notificação do Advisor devem ser enviados (p.ex. - Sent_Server@myserver.com).
    - Senha Global do Sistema – digite uma senha e a senha de confirmação correspondente. Esta será a senha de todos os usuários padrão. Isso inclui o usuário do sistema operacional esecadm e os usuários dos bancos de dados. Consulte o Banco de Dados do Sentinel, na seção Pós-instalação do Sentinel 5 para Oracle, para obter a lista de usuários padrão do banco de dados criada durante a instalação.
    - Diretório de Dados – o local dos arquivos de dados do Banco de Dados. Para mudar o local padrão, clique no botão ... e selecione um local. O padrão é $ESEC_HOME/data.

NOTA: O Diretório de Dados precisa permitir gravação pelo usuário do Oracle. Para isso, execute os comandos a seguir como Usuário Root:

```
chown –R oracle:dba <directory_path>
chmod –R 770 <directory_path>
```

supondo que "oracle" é seu nome de usuário no Oracle e que "dba" e seu nome de grupo no Oracle.

NOTA: Se estiver instalando o Advisor, a opção de instalação Simples irá configurar o Advisor para que use o Download Direto da Internet com um intervalo de atualização de 12 horas e todas as notificações de e-mail habilitadas.

- Para instalar o Advisor, selecione *Instalar Consultor*. Digite um nome de usuário e senha. Se o nome de usuário ou senha não puder ser verificado, após clicar em *Avançar* você será perguntado se deseja continuar (não recomendado). Se optar por continuar, digite a senha do Advisor novamente na janela de confirmação de senha. Caso contrário, corrija a senha do Advisor.

Clique em *Avançar*.

Número de Série: | Chave de Licença:

Servidor SMTP: localhost | E-mail: esecadm

Senha Global do Sistema (usada para todos os usuários do Sentinel e o Gerenciador de Coletor)

Senha: | Confirmar Senha:

Diretório de Dados: C:\Archivos de programa\sentinel5.1.3.0\data ...

Instalar Consultor (digite o nome de usuário/senha abaixo)

Nome de Usuário: | Senha:

13. Digite as informações sobre a configuração do banco de dados:
    - Nome do Banco de Dados – O nome da instância de banco de dados Oracle para a criação e instalação de objetos do Banco de Dados do Sentinel. Não pode já existir um banco de dados com esse nome.
    - Arquivo de Driver do Oracle JDBC. Esse é o caminho completo para o arquivo .jar, normalmente $ORACLE_HOME/jdbc/lib/ojdbc14.jar (não é possível usar variáveis de ambiente nesse campo).

14. Clique em *OK* no nome de usuário do Oracle padrão.

15. Leia as informações apresentadas nas telas que aparecerem e clique em *Avançar* ao concluir. Depois de concluída a instalação, será necessário reinicializar o sistema.

NOTA: Caso deseje instalar algum software de Integração de Terceiros (Suporte técnico HP ou Integração do Remedy), após a reinicialização da máquina, execute o instalador novamente e selecione o software de Integração de Terceiros a ser instalado. Para obter mais informações, consulte o *Guia de Integração de Terceiros*.

16. O instalador do Sentinel desliga o Registro de Arquivos por padrão. Para fins de recuperação de bancos de dados, é altamente recomendável que, após a instalação e antes de começar a receber dados de eventos de produção, você habilite o Registro de Arquivos. Você também deve programar um backup dos seus registros de arquivo para liberar espaço no destino do registro de arquivos, do contrário o banco de dados irá parar de aceitar eventos.

Instalação Personalizada no Linux

Como realizar uma Instalação Personalizada

1. Verifique se você coletou as informações, realizou as tarefas e atendeu aos requisitos especificados na seção Pré-instalação do Sentinel 5 para Oracle em relação aos componentes que está instalando.
2. Verifique a configuração do Oracle no Linux.
3. Faça login como usuário Root.
4. Insira e monte o CD de instalação do Sentinel.
5. Para iniciar o programa de instalação, vá para o diretório de instalação no CD-ROM e digite:

   Para o modo de interface gráfica:

   ```
   ./setup.sh
   ```

   ou

   Para modo textual:

   ```
   ./setup.sh –console
   ```

6. Clique na seta para baixo e selecione uma das seguintes opções de idioma:
   - Inglês
   - Francês
   - Alemão
   - Italiano
   - Português
   - Espanhol
7. Depois de ler a tela de boas-vindas, clique em *Avançar*.
8. Aceite o Contrato de Licença de Usuário Final e clique em *Avançar*.
9. Aceite o diretório de instalação padrão ou clique em *Procurar* para especificar o local da instalação. Clique em *Avançar*.

10. Selecione *Personalizado* (padrão). Clique em *Avançar*.
11. Selecione os recursos a serem instalados.

NOTA: Para obter mais informações sobre os componentes que podem ser instalados e em que locais para diferentes configurações, consulte o *Capítulo 1, Requisitos do Sistema*.

As opções a seguir estão disponíveis:

- Banco de Dados – instala o Banco de Dados do Sentinel.
- Servidor de Comunicação – instala o barramento de mensagens (iSCALE)
- Consultor
- Mecanismo de Correlação
- DAS
- Serviço do Coletor
- Sentinel Control Center
- Gerenciador de Dados do Sentinel
- HP OpenView Service Desk**
- Integração do Remedy**

NOTA: **Para obter informações sobre a instalação do HP OpenView Service Desk ou da Integração do Remedy, consulte o *Guia de Integração de Terceiros*.

NOTA: Se nenhum dos recursos filhos de "Serviços do Sentinel" for selecionado, anule a seleção do recurso "Serviços do Sentinel" também. Ele ficará esmaecido com uma marca de seleção se ainda estiver selecionado, mas todos os recursos filho serão desmarcados.

NOTA: Como parte da instalação do componente Banco de Dados de Sentinel, o instalador irá colocar arquivos na pasta $ESEC_HOME/utilities/db.

---

12. Se você selecionou a instalação do DAS, será solicitado a fornecer:
    - Número de Série
    - Chave de Licença
13. Se você selecionou a instalação de qualquer componente de integração de terceiros, será solicitado a fornecer uma senha para desbloquear o(s) componente(s) de integração de terceiros selecionados. Para obter mais informações, consulte o *Guia de Integração de Terceiros*.
14. Especifique o nome de usuário do Administrador do Sentinel no sistema operacional e o local do diretório pessoal. Esse é o nome de usuário que terá a propriedade do produto Sentinel instalado. Se o usuário não existir ainda, um usuário será criado com um diretório pessoal no diretório especificado.
    - Nome de usuário do Administrador do sistema operacional – O padrão é esecadm
    - Diretório pessoal do Administrador do sistema operacional – O padrão é "/export/home". Se o nome de usuário for esecadm, o diretório pessoal do usuário será /export/home/esecadm.

NOTA: Se um novo usuário for criado, sua senha precisará ser definida manualmente, separadamente desse instalador. O Sentinel recomenda que isso seja feito diretamente pelo registro no sistema após a instalação do produto.

Para obedecer as rígidas configurações de segurança exigidas pela Certificação de Critérios Comuns, o Sentinel exige uma senha forte com as seguintes características:

1. Escolha senhas com no mínimo 8 caracteres, que incluam ao menos um dígito em MAIÚSCULA, um em minúscula, um símbolo especial (#$_) e um dígito numérico (0-9). Não use espaços.

2. A senha não pode conter o nome usado no e-mail nem partes do nome completo.

3. A senha não deve ser uma palavra "comum" (por exemplo, não deve ser uma palavra registrada em dicionário nem gíria de uso comum).

4. A senha não deve conter palavras de idioma algum, pois existem vários programas de invasão de senha capazes de verificar milhões de possibilidades de combinações de palavras em segundos.

5. Escolha uma senha de que possa se lembrar, mas que seja complexa. Por exemplo, Mft5#AIdade (Meu filho tem 5 anos de idade) OU EmnCh5#a (Eu moro na Califórnia há 5 anos).

15. Se optar por instalar o Sentinel Control Center, aparecerá um prompt de tamanho de heap JVM (Java Virtual Machine):
    - Tamanho de heap JVM (MB) - Por padrão, é definido como metade do tamanho da memória física detectada na máquina, com um máximo de 1024 MB. Esse será o tamanho de heap JVM máximo usado somente pelo Sentinel Control Center.

16. Se você optar por instalar o Serviço do Coletor, escolha proteger ou não proteger o Gerenciador do Coletor do Assistente com uma senha. Se você optar por proteger o Gerenciador do Coletor do Assistente, será solicitado a criar uma senha para ele.

NOTA: Para a proteção do Coletor do Assistente com uma senha, será necessário digitar essa senha ao fazer o upload, download ou depuração de Coletores nesse Gerenciador do Coletor do Assistente. Essa senha complementa o nome de usuário e senha do Sentinel necessários para fazer o login Construtor de Coletor do Assistente.

NOTA: Para obedecer as rígidas configurações de segurança exigidas pela Certificação de Critérios Comuns, o Sentinel exige uma senha forte com as seguintes características:

1. Escolha senhas com no mínimo 8 caracteres, que incluam ao menos um dígito em MAIÚSCULA, um em minúscula, um símbolo especial (!@#$%^&*()_+), e um dígito numérico (0-9).

2. A senha não pode conter o nome usado no e-mail nem partes do nome completo.

3. A senha não deve ser uma palavra "comum" (por exemplo, não deve ser uma palavra registrada em dicionário nem gíria de uso comum).

4. A senha não deve conter palavras de idioma algum, pois existem vários programas de invasão de senha capazes de verificar milhões de possibilidades de combinações de palavras em segundos.

5. Escolha uma senha de que possa se lembrar, mas que seja complexa. Por exemplo, Mft5#AIdade (Meu filho tem 5 anos de idade) OU EmnCh5#a (Eu moro na Califórnia há 5 anos).

Opções de proteção por senha do Gerenciador de Coletor:

Don't password protect this Collector Manager

Password protect this Collector Manager

Palavra-passe:

Confirmar Senha:

17. Se optar por instalar o DAS, selecione a quantidade de RAM do sistema que deseja alocar para o Serviço de Acesso a Dados. No caso de ambientes distribuídos, recomenda-se selecionar o máximo de memória (4 GB). No caso de ambientes independentes, recomenda-se selecionar metade da memória RAM.

18. Para a instalação do banco de dados, será solicitado o seguinte:
    a. Selecione a plataforma do servidor do banco de dados de destino como Oracle 9i e selecione uma das ações a seguir:
        - Criar um novo banco de dados com objetos de banco de dados – cria uma nova instância de banco de dados Oracle e preenche a nova instância com objetos de banco de dados.

- Adicionar objetos de banco de dados a um banco de dados vazio existente – somente adiciona um banco de dados a uma instância de banco de dados Oracle existente. A instância de banco de dados Oracle existente precisa estar vazia, exceto pela presença do usuário esecdba.

b. Digite o diretório de registro de instalação do banco de dados (padrão: $ESEC_HOME/logs/db). Aceite o 'Diretório do registro de instalação do banco de dados' padrão ou clique em *Procurar* para especificar um local diferente.

Selecione a plataforma do servidor do banco de dados de destino:

Oracle 9i

Criar um novo banco de dados com objetos de banco de dados.

Adicionar objetos de banco de dados a um banco de dados vazio existente.

Diretório do registro de instalação do banco de dados:

/opt/sentinel5.1.3.0/logs/db

Procurar

c. Clique em *OK* no nome de usuário do Oracle padrão.

d. Se você optar por criar um novo banco de dados, digite o seguinte:

- O caminho para o arquivo de driver do Oracle JDBC (o nome típico do arquivo .jar é ojdbc14.jar). Esse é o caminho completo para o arquivo .jar, normalmente $ORACLE_HOME/jdbc/lib/ojdbc14.jar (não é possível usar variáveis de ambiente nesse campo).
- Nome de host – O nome de host da máquina onde o banco de dados será instalado. Esse campo não é configurável se uma nova instância de banco de dados estiver sendo criada.
- Nome do Banco de Dados – O nome da instância de banco de dados que será instalada.

e. Se você optou por adicionar objetos de bancos de dados a um banco Oracle vazio existente, será solicitado a fornecer as informações a seguir.

- O caminho para o arquivo de driver do Oracle JDBC (o nome típico do arquivo .jar é ojdbc14.jar). Esse é o caminho completo para o arquivo .jar, normalmente $ORACLE_HOME/jdbc/lib/ojdbc14.jar (não é possível usar variáveis de ambiente nesse campo).

- Nome de host do banco de dados ou endereço IP – O nome ou endereço IP do host onde está o banco de dados Oracle ao qual você deseja adicionar objetos de banco de dados. Pode ser o nome de host local ou um nome de host remoto.
- Nome do banco de dados – O nome da instância do banco de dados Oracle vazio existente à qual você deseja adicionar objetos de banco de dados (o padrão é ESEC). Esse nome de banco de dados precisa aparecer como nome de um serviço no arquivo tnsnames.ora (no diretório $ORACLE_HOME/network/admin/) da máquina onde o instalador está sendo executado.

NOTA: Se o nome do banco de dados não estiver no arquivo tnsnames.ora, o instalador não exibirá um erro nesse momento da instalação (porque ele verifica a conexão usando uma conexão JDBC direta), mas a instalação do Banco de dados irá falhar quando o instalador tentar se conectar ao banco de dados por meio de sqlplus. Se a instalação do banco de dados falhar nesse ponto, modifique o nome do serviço desse banco de dados no arquivo tnsnames.ora nessa máquina, sem sair do instalador, retroceda uma tela no instalador e avance novamente. Será feita uma nova tentativa de instalação do banco de dados com os novos valores no arquivo tnsnames.ora.

- Porta do banco de dados (o padrão é 1521).
- Para o usuário Administrador do Banco de Dados do Sentinel (DBA), especifique a senha do usuário "esecdba". O campo de nome de usuário desse prompt não é editável.

f. Se você optou por criar um novo banco de dados, verá o prompt a seguir:

- Memória Oracle (MB) – A quantidade de memória RAM a ser alocada a essa instância de banco de dados Oracle.
- Porta de Escuta – a porta onde criar uma escuta Oracle (o padrão é 1521).
- Senha e confirmação de senha do usuário SYS – SYS é um usuário do Oracle padrão que será criado na nova instância de banco de dados. A senha desse usuário será definida como o valor especificado aqui.
- Senha e confirmação de senha do usuário SYSTEM – SYSTEM é um usuário do Oracle padrão que será criado na nova instância de banco de dados. A senha desse usuário será definida como o valor especificado aqui.

g. Se você optar por criar um novo banco de dados, será solicitado a digitar o tamanho do banco: Você tem as opções a seguir:

- Padrão (20 GB)
- Grande (400 GB)
- Personalizado (especifique manualmente o tamanho). Se você escolher essa opção, será solicitado a fornecer:
  - o tamanho inicial de cada arquivo de banco de dados em MB (100 a 10.000)
  - o tamanho máximo de cada arquivo de banco de dados em MB (2.000 a 100.000)
  - o tamanho de todos os arquivos de banco de dados em MB (7.000 a 2.000.000)
  - o tamanho de cada arquivo de registro em MB (100 a 100.000)

Please select Standard, Large, or Custom database size.

(•) Standard (20,000MB, 30 day capacity @ 500,000 events per day)

( ) Large (400,000MB, 30 day capacity @ 10,000,000 events per day)

( ) Custom (specify database sizing manually)

h. Se você optar por criar um novo banco de dados, será solicitado a digitar o local de armazenamento dos arquivos de bancos de dados a seguir:

NOTA: Para fins de recuperação e desempenho, recomenda-se que esses locais estejam em dispositivos de E/S diferentes.

Como o instalador não irá criar esses diretórios, eles precisam ser criados externamente antes de avançar.

Esses diretórios precisam permitir gravação pelo usuário do Oracle. Para tornar esses diretórios graváveis pelo usuário do Oracle, execute os comandos a seguir para cada diretório como Usuário Root:

```
chown –R oracle:dba <directory_path>
chmod –R 770 <directory_path>
```

supondo que "oracle" é seu nome de usuário no Oracle e que "dba" e seu nome de grupo no Oracle.

- Diretório de dados
- Diretório de índices
- Diretório de Dados de Resumo
- Diretório de Índices de Resumo
- Diretório Temporário e Desfazer Tabela:
- Diretório A do Membro de Redo Log
- Diretório B do Membro de Redo Log

i. Se você optou por criar um novo banco de dados, digite as informações de autenticação do Administrador do Banco de Dados do Sentinel (DBA). Este é o esecdba, o proprietário dos objetos de banco de dados.

j. Digite as informações de autenticação do usuário do banco de dados do aplicativo Sentinel. Este é o esecapp, o nome do usuário do aplicativo Sentinel que os processos do Sentinel usam para a conexão com o banco de dados.

k. Digite as informações de autenticação do usuário do Banco de Dados do Administrador do Sentinel. Este é o esecadm, o usuário Administrador do Sentinel.

l. Clique em *Avançar* na janela de resumo da instalação do banco de dados.

19. Se você optou por instalar o DAS, mas não optou por instalar o Banco de Dados do Sentinel, será solicitado a fornecer as informações do Banco de dados do Sentinel para Oracle a seguir. Essas informações serão usadas para configurar o DAS para que aponte para o Banco de Dados do Sentinel.
    - Nome de host do banco de dados ou endereço IP – O nome ou endereço IP do Banco de Dados do Sentinel para Oracle a ser configurado para se conectar ao componente DAS.
    - Nome do banco de dados – O nome da instância de banco de dados Oracle vazia a ser configurada para se conectar ao componente DAS (o padrão é ESEC).
    - Porta do banco de dados (o padrão é 1521).
    - Para o Usuário do Banco de Dados do Aplicativo Sentinel, especifique o login "esecapp" e digite a senha dada para esse usuário durante a instalação do Banco de Dados do Sentinel.

20. Se você optou por instalar o DAS, configure o suporte de e-mail do Sentinel. Especifique o servidor SMTP e o endereço de e-mail do remetente a ser usado pelo Serviço de Execução para enviar mensagens (opcional – você pode editar isso manualmente após instalar [$ESEC_HOME\sentinel\config\execution.properties]):

SMTP Server:

"From" Email Address:

21. Se você optou por instalar o Advisor, selecione o tipo de instalação (se a opção Consultor foi escolhida, um nome de usuário e senha)
    - Download Direto da Internet - A máquina do Advisor está diretamente conectada à Internet. Nessa configuração, é feito o download automático das atualizações do Sentinel da Internet com regularidade.
    - Independente - O Advisor é configurado como um sistema isolado que requer intervenção manual para receber uma atualização do Sentinel.
22. Se você optou por instalar o Advisor e selecionou o uso do Download Direto da Internet, digite seu nome de usuário, senha e freqüência de atualização dos dados do Advisor. Se o nome de usuário ou senha não puder ser verificado, após clicar em *Avançar* você será perguntado se deseja continuar (não recomendado). Se optar por continuar, digite a senha do Advisor novamente na janela de confirmação de senha. Caso contrário, corrija a senha do Advisor.

Please enter the username and password to access the Advisor server and feed data:

Username:

Password:

Please select how often Advisor data needs to be updated:

6 Hours   12 Hours

23. Se você optou por instalar o Advisor, digite:
    - Endereço do remetente, que será exibido nas notificações de e-mail
    - Endereço do destinatário para o envio de notificações por e-mail

---

NOTA: Após a instalação, para mudar os endereços de e-mail do Advisor, edite os arquivos attackcontainer.xml e alertcontainer.xml no diretório $ESEC_HOME/sentinel/config. Para obter mais informações, consulte o *Capítulo 7 – Guia Consultor do Guia do Usuário do Sentinel*.

    - Selecione *Sim* ou *Não* para o recebimento de e-mails sobre atualizações bem sucedidas do Advisor. As notificações de erro serão sempre enviadas.

Advisor Configuration

Enter the from address for sending the email notifications: Advisor

Enter the addresses to which email notifications should be sent (comma separated): esecadm

Do you want email notifications for successful Advisor updates (error notifications will always be sent)?

Yes   No

24. Se você optou por instalar o HP Service Desk ou a Integração do Remedy, será solicitado a fornecer informações adicionais. Para obter mais informações, consulte o *Guia de Integração de Terceiros do Sentinel*.
25. Leia as informações apresentadas nas telas que aparecerem e clique em *Avançar* ao concluir. Depois de concluída a instalação, será necessário reinicializar. Clique em *Concluir* para reinicializar o sistema.
26. O instalador do Sentinel desliga o Registro de Arquivos por padrão. Para fins de recuperação de bancos de dados, é altamente recomendável que, após a instalação e antes de começar a receber dados de eventos de produção, você habilite o Registro de Arquivos. Você também deve programar um backup dos seus registros de arquivo para liberar espaço no destino do registro de arquivos, do contrário o banco de dados irá parar de aceitar eventos.
27. Se você espera uma taxa de eventos elevada (superior a 500 eventos por segundo), é necessário seguir as instruções de configuração adicionais contidas na seção Configurando a Estratégia de Inserção de Eventos da Interface de Chamada Oracle (OCI).

Instalando o Sentinel Control Center e o Construtor de Coletor no Windows

Instalando o Sentinel Control Center e o Construtor de Coletor no Windows

1. Insira o CD de instalação do Sentinel na unidade de CD-ROM.
2. Procure o CD e clique duas vezes em *setup.bat*.

NOTA: Não há suporte para a instalação no modo de console no Windows.

3. Depois de ler a tela de boas-vindas, clique em *Avançar*.
4. Aceite o Contrato de Licença de Usuário Final e clique em *Avançar*.
5. Aceite o diretório de instalação padrão ou clique em *Procurar* para especificar o local da instalação. Clique em *Avançar*.

Nome do directório:

/opt/sentinel5.1.3.0

Procurar

6. Selecione os recursos a serem instalados.
7. Digite o endereço do host e a porta em que o Servidor de Comunicação está instalado.

Host (hostname or IP address):

<host name or IP Address>

Port (default = 10012):

10012

8. Se optou por instalar o Sentinel Control Center, aparecerá um prompt de tamanho de heap JVM (Java Virtual Machine):
   - Tamanho de heap JVM (MB) - Por padrão, é definido como metade do tamanho da memória física detectada na máquina, com um máximo de 1024 MB. Esse será o tamanho de heap JVM máximo usado somente pelo Sentinel Control Center.

Clique em *Avançar*.

9. Clique em *Instalar*.
10. Leia as informações apresentadas nas telas que aparecerem e clique em *Avançar* ao concluir. Clique em *Concluir*.

Pós-instalação do Sentinel 5 para Oracle

Atualizando o e-mail do Sentinel para autenticação SMTP

Se o sistema exigir autenticação SMTP, você precisará atualizar o arquivo execution.properties. Esse arquivo está na máquina em que o DAS foi instalado. Ele está localizado em $ESEC_HOME/sentinel/config. Para configurar esse arquivo, execute mailconfig.sh para mudar o arquivo e mailconfigtest.sh para testar as mudanças.

Para configurar o arquivo execution.properties

1. Na máquina em que o DAS foi instalado, faça login como esecadm e mude para o diretório:

```
$ESEC_HOME/sentinel/config
```

2. Execute mailconfig desta maneira:

```
./mailconfig.sh -host <servidor SMTP> -from <endereço de
   e-mail de origem> -user <usuário de autenticação de e-
   mail> –password
```

Exemplo:

```
./mailconfig.sh -host 10.0.1.14 -from
   meu_nome@domínio.com -user meu_nome_de_usuário –
   password
```

Depois de digitar esse comando, você será solicitado a fornecer uma nova senha.

```
Digite a senha:*********

Confirme a senha:*********
```

NOTA: Ao usar a opção password, ela deve ser o último argumento.

Para testar a configuração de execution.properties

1. Na máquina em que o DAS foi instalado, faça login como esecadm e mude para o diretório:

```
$ESEC_HOME/sentinel/config
```

2. Execute mailconfigtest desta maneira:

```
./mailconfigtest.sh -to <endereço de e-mail de destino>
```

Se o e-mail for enviado com êxito, será exibida a seguinte saída na tela e o e-mail será recebido no endereço de destino.

```
O e-mail foi enviado com êxito!
```

Verifique a caixa de correio do e-mail de destino para confirmar o recebimento da mensagem. A linha de assunto e o conteúdo devem ser:

```
Assunto: Testando a propriedade de e-mail do Sentinel

Este é um teste da configuração da propriedade de e-mail
   do Sentinel. Se você vir esta mensagem, a propriedade
   de e-mail do Sentinel foi configurada corretamente
   para enviar e-mail
```

Banco de Dados do Sentinel

Após instalar o Banco de Dados do Sentinel, o banco irá conter os usuários padrão a seguir:

- esecdba – Proprietário do esquema de bancos de dados. O privilégio de DBA não é concedido ao usuário esecdba por questões de segurança. Para usar o Enterprise Manager, crie um usuário com privilégios de DBA.
- esecapp – Usuário do aplicativo de banco de dados. Este é o usuário do aplicativo utilizado para a conexão com o banco de dados.
- esecadm – Usuário do banco de dados que é o Administrador do Sentinel. Não é a mesma conta do usuário do sistema operacional esecadm.
- esecrpt – Usuário do relatório de bancos de dados
- SYS – Usuário do banco de dados SYS
- SYSTEM – Usuário do banco de dados SYSTEM

Serviço do Coletor

Durante a instalação do Serviço do Coletor, os seguintes Coletores serão instalados, cada qual com uma configuração de porta para sua execução.

Produto	Nome do Coletor
Coletores Demo	
Teste de upload de bens, funciona com o Coletor DemoEvents	DemoAssetUpload
Teste de eventos demo, funciona com o Coletor DemoAssetUpload e com o DemoVulnerabilityUpload	DemoEvents
Teste de upload de vulnerabilidade, funciona com o Coletor DemoEvents	DemoVulnerabilityUpload
Teste de envio de um evento	SendOneEvent
Teste de envio de vários eventos	SendMultipleEvents

NOTA: Para obter mais informações sobre a configuração dos Coletores Demo, consulte o *Capítulo 12 - Teste da Instalação.*

NOTA: Para Coletores adicionais, vá até o Sentinel Customer Portal para obter o Service Pack mais recente para a versão que foi instalada. O Service Pack mais recente para a versão em uso irá conter o conjunto completo dos Coletores mais recentes disponíveis para a verão do Sentinel em uso.

Para obter mais informações (inclusive sobre configuração) consulte a documentação que acompanha cada Coletor em:

$WORKBENCH_HOME/Elements/<nome do Coletor>/Docs/

Para instalar Coletores adicionais, execute o script do Service Pack no CD do Service Pack.. O script irá instalar os Coletores em nível local.

No Windows:

```
.\service_pack.bat
```

No UNIX:

```
./service_pack.sh
```

Para obter as instruções de instalação do Service Pack e uma lista de Coletores, consulte as *notas do Service Pack Release*.

Atualizando a Chave de Licença

Como atualizar a chave de licença (Linux)

1. Faça login como usuário esecadm.
2. Insira e monte o CD de instalação do Sentinel.
3. use o comando cd para mudar para disk1/utilities/linux:
4. Digite o seguinte comando:

    ```
    ./softwarekey
    ```

5. Digite o número 1 como a chave principal. Pressione Enter.

Criando uma Instância Oracle para o Banco de Dados do Sentinel

NOTA: Esse procedimento é apresentado a título de exemplo caso você deseje criar tabelas próprias em comparação com o uso do recurso de criação de tabelas do CD de instalação. Os valores de tamanho podem variar dependendo da configuração e dos requisitos do sistema. Os nomes das tabelas devem seguir exatamente as especificações abaixo.

Na instância Oracle, será necessário configurar:

- parâmetros
- tabelas

Criando uma Instância Oracle

1. Faça login como usuário Oracle.
2. Use a interface gráfica do Assistente de Banco de Dados Oracle para criar o seguinte:

NOTA: Os valores podem variar dependendo da configuração e dos requisitos do sistema.

Parâmetros Mínimos Recomendados para Configuração do Linux	
Parâmetros	**Tamanho (bytes ou outra especificação)**
db_cache_size	1 GB
java_pool_size	33,554,432
large_pool_size	8,388,608
shared_pool_size	100 MB
pga_aggregate_target	150,994,944
sort_area_size	109,051,904
open_cursors	500
cursor_sharing	SIMILAR
hash_join_enabled	TRUE
optimizer_index_caching	50
optimizer_index_cost_adj	55

Tamanho Mínimo Recomendado para Tabela do Linux		
Tabela	**Tamanho de Exemplo**	**Notas**
REDO	3 x 100M	Este é o valor mínimo. Você deve criar redo logs maiores se tiver um EPS elevado.
SYSTEM	500M	Valor mínimo
TEMP	1G	Valor mínimo
UNDO	1G	Valor mínimo
ESENTD	5G	Valor mínimo Este é para dados de eventos
ESENTD2	500M	Valor mínimo Dados de configuração, bens, vulnerabilidade e associações (autoextend habilitado)
ESENTWFD	250M	Para dados do iTrac (autoextend habilitado)
ESENTWFX	250M	Para índice do iTrac (autoextend habilitado)
ESENTX	3G	Valor mínimo Para índice de eventos
ESENTX2	500M	Valor mínimo Índice de configuração, bens, vulnerabilidade e associações (autoextend habilitado)
SENT_ADVISORD	200M	Valor mínimo Para dados do Advisor (autoextend habilitado)
SENT_ADVISORX	100M	Valor mínimo Para índice do Advisor (autoextend habilitado)
SENT_LOBS	100M	Valor mínimo Para objetos grandes de bancos de dados (autoextend habilitado)
SENT_SMRYD	3G	Valor mínimo Para dados de resumo de Agregação
SENT_SMRYX	2G	Valor mínimo Para índice de resumo de Agregação

3. Execute o script createEsecdba.sh encontrado no diretório sentinel\dbsetup\bin no CD de Instalação do Sentinel. Este script irá criar o usuário esecdba, que é necessário para adicionar objetos de bancos de dados com o uso do instalador do Sentinel.
4. Faça um backup do banco de dados.

Configurando a Estratégia de Inserção de Eventos da Interface de Chamada Oracle (OCI)

O Sentinel 5.1 oferece uma estrutura para a inclusão de diferentes estratégias para a inserção de eventos no banco de dados. O Sentinel 5.1 oferece duas estratégias para a inserção de eventos no banco de dados Oracle.

- JDBCLoadStrategy
- OCILoadStrategy

A estratégia a ser usada para a inserção de eventos é regida pela propriedade da estratégia de inserção do componente EventStoreService do arquivo das_binary.xml.

A estratégia JDBC é a estratégia padrão configurada out of the box.

A estratégia OCI é uma estratégia de inserção nativa para a agilização da inserção de eventos. Essa estratégia requer que as bibliotecas OCI do Oracle estejam instaladas na máquina que está executando o componente DAS. A estratégia OCI precisa ser usada em configurações para as quais é esperada uma alta taxa de eventos.

O número de eventos a ser agrupado para inserção no banco de dados é regido pela propriedade insert.batchsize. Essa propriedade insert.batchsize é usada por todas as estratégias de inserção de eventos.

Para mudar a estratégia de inserção de eventos do Sentinel da Estratégia de Inserção JDBC padrão para a Estratégia de Inserção OCI, há algumas etapas que precisam ser executadas.

Mudando a estratégia de inserção de eventos da Estratégia JDBC para a OCI.

1. Verifique se as bibliotecas OCI do Oracle estão instaladas na máquina que está executando o componente DAS do Sentinel. Você precisará saber o caminho para o ORACLE_HOME nas etapas a seguir.
2. Faça login na máquina partindo da etapa 1 como o usuário esecadm.
3. Crie um arquivo ".bash_profile" no diretório pessoal do usuário esecadm. Coloque o texto a seguir nesse arquivo (modifique o caminho para o ORACLE_HOME para que corresponda à sua instalação):

```
ORACLE_HOME=/build/home/oracle/OraHome
export ORACLE_HOME
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$ORACLE_HOME/lib
export LD_LIBRARY_PATH
```

4. Abra o arquivo $ESEC_HOME/sentinel/config/das_binary.xml para editá-lo em qualquer editor de texto.

5. Faça uma pesquisa no texto a seguir:

   ```
   JDBCLoadStrategy
   ```

6. Mude esse texto para:

   ```
   OCILoadStrategy
   ```

7. Grave esse mudança no arquivo das_binary.xml.
8. Reinicie o aplicativo binário DAS. (É fácil reiniciar o Binário DAS realizando um "ps –ef | grep DAS_Binary" para obter o ID do processo, eliminando esse processo e em seguida permitindo que o Watchdog do Sentinel automaticamente reinicie o processo.)

   Após o reinício do Binário DAS, a biblioteca $ESEC_HOME/sentinel/lib/libocievent.so será carregada e usada para realizar as inserções de Eventos no banco de dados via OCI.

Opções adicionais de Inserção de Eventos OCI

Além de especificar a "OCILoadStrategy" no arquivo das_binary.xml, há várias outras opções relacionadas a OCI que também podem ser configuradas.

- insert.batchsize – Essa definição permite configurar o máximo número de Eventos para inserção no banco de dados de uma só vez.
- insert.oci.workerCount – Essa definição permite configurar o número de threads usadas para inserir dados de Eventos no banco de dados.
- insert.oci.queueWaitTime – Essa configuração especifica o tempo máximo, em segundos, para aguardar antes de inserir os dados da fila de entrada no banco de dados. Sempre que um "tamanho de lote" de eventos é recebido, o lote inteiro é inserido. Mas o fluxo de entrada de eventos é lento, o tempo de espera da fila é usado para determinar o momento da inserção no banco de dados (mesmo que um lote completo de eventos ainda não tenha sido recebido).
- insert.oci.highWatermark – A alta marca d’água da fila do Evento de entrada.
- insert.oci.lowWatermark – A marca d’água baixa da fila do Evento de entrada.
- insert.oci.optimizationFlag – Flag de otimização. "ligada" ou "desligada".

Dicas de Depuração de OCI

A interface OCI irá registrar mensagens no arquivo $ESEC_HOME/sentinel/log/ocievent.log. As mensagens iniciais gravadas no arquivo de registro devem incluir mensagens de conexão de banco de dados bem sucedidas (ou fracassadas)… Este é um bom local para verificar se a biblioteca OCI foi carregada e configurada corretamente.

A interface OCI também irá registrar erros no arquivo das_binary localizado no diretório $ESEC_HOME/sentinel/log. Os erros registrados no arquivo de registro das_binary log incluem falhas na localização/carregamento da biblioteca libocievent.so, falhas de conexão ao banco de dados e falhas de inserção de Associações de Eventos/Evento.

Se houver mensagens de erro indicando que o arquivo "libocievent.so" não está sendo localizado ou carregado, então há três coisas a serem verificadas:

1. Verifique se as bibliotecas OCI Oracle estão instaladas.
2. Verifique se o arquivo "libocievent.so" está localizado no diretório $ESEC_HOME/sentinel/lib.

3. Verifique se o diretório $ESEC_HOME/sentinel/lib está no caminho "LD_LIBRARY_PATH" do usuário "esecadm". Em caso negativo, você pode atualizar o caminho LD_LIBRARY_PATH no perfil do usuário "esecadm".
4. Verifique se as variáveis de ambiente ORACLE_HOME e LD_LIBRARY_PATH estão atualizadas corretamente nas variáveis de ambiente do usuário esecadm conforme descrito na seção "Mudando a estratégia de inserção de eventos da Estratégia JDBC para a OCI".

5 Instalando o Sentinel 5 para MS SQL

NOTA: O termo Agente é sinônimo de Coletor. De agora em diante, Agentes serão referidos como Coletores.

Este capítulo descreve a instalação do Sentinel Enterprise Security Management Sentinel 5 para MS SQL.

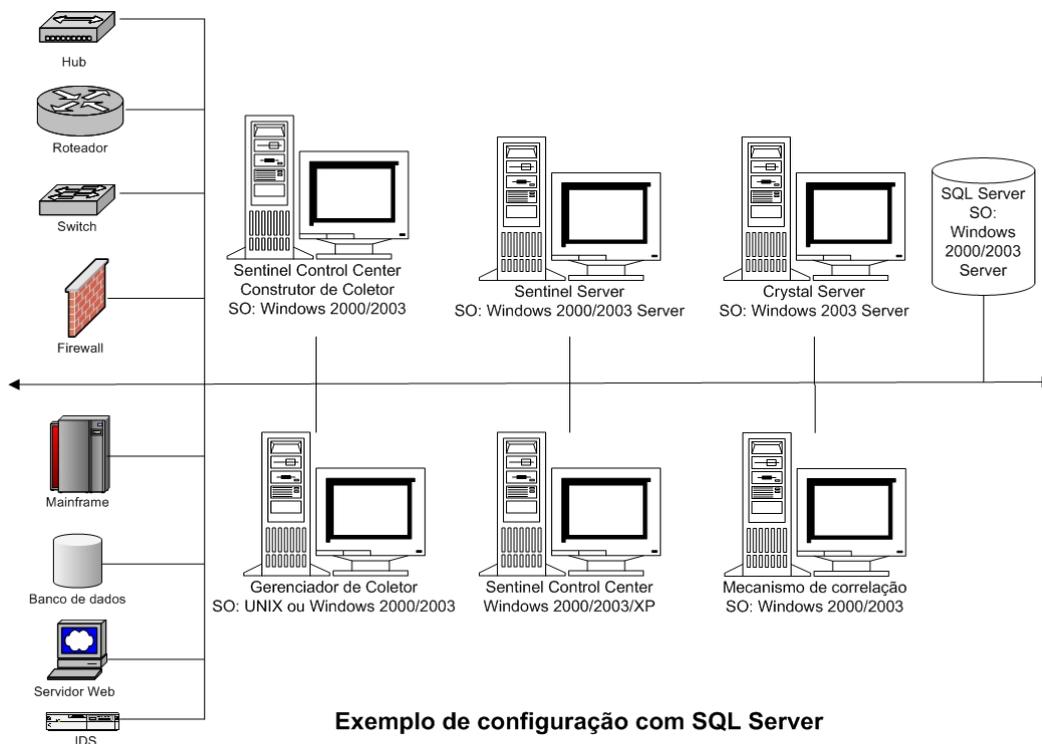
Pré-instalação do Sentinel 5 para MS SQL

NOTA: Antes da instalação, verifique se as máquinas atendem aos requisitos mínimos do sistema e se o sistema operacional foi "reforçado" com o uso das atuais melhores práticas de segurança.

NOTA: O Sentinel não oferece suporte ao MS cluster ou Alta Disponibilidade para Windows.

NOTA: Ao realizar uma instalação limpa do Sentinel depois de ter instalado uma versão anterior do Sentinel, é necessário remover determinados arquivos e configurações do sistema que podem ter sobrado de uma instalação anterior. Se esses arquivos ou configurações não forem removidos, pode haver falha de uma nova instalação limpa. Isso deve ser feito em cada máquina onde esteja sendo feita uma instalação limpa. Para obter mais informações, veja o *Apêndice E*.

A seguir está uma típica configuração para o Sentinel:
A configuração pode ser diferente, dependendo do ambiente. Independentemente da configuração escolhida, é necessário instalar o banco de dados primeiro.

Exemplo de configuração com SQL Server

NOTA: Para obter mais informações sobre os sistemas operacionais suportados, consulte o *Capítulo 1 – Introdução, Plataformas Suportadas para o Sentinel Server no Windows*.

Obtendo uma Chave de Licença

O Serviço de Acesso a Banco de Dados (DAS) do Sentinel Server exige que haja uma chave de licença válida para instalar e executar o serviço. Essa chave de licença é bloqueada para a máquina onde o DAS será instalado. Uma chave de licença emitida para uma máquina não funciona em outra máquina.

Para obter a chave de licença, é necessário determinar o número do ID de host e fornecer essa informação para a Novell, que atribuirá uma chave de licença.

Para determinar o ID de host

1. Insira o CD de instalação do Sentinel na unidade de CD-ROM.
2. Procure o diretório de utilitários no CD.
3. Execute o arquivo executável:

```
hostid.exe
```

4. Envie esse número de ID do host para o Suporte Técnico da Novell. Eles forecerão a você uma chave de licença.

Banco de dados do Sentinel

Antes de instalar o Sentinel Server, será necessário:

- Para obter os requisitos de hardware, consulte os *Capítulos 1 e 2*
- Servidor Windows 2000 com Service Patch 4 ou Servidor Windows 2003 com Service Patch1
- Servidor SQL 2000 Enterprise Edition Service Pack 3a ou Servidor SQL 2005 Enterprise Addition (Sentinel v5.1.1 SP1 e posteriores) instalado e em execução.

  NOTA: Por motivos de desempenho, é ALTAMENTE recomendável que, dependendo de se tratar da instalação em RAID, e se o ambiente RAID permitir, o Registro de Transação deve apontar para o disco de gravação mais rápido que estiver disponível.

  NOTA: Se você instalou o Servidor SQL com autenticação de modo misto, poderá usar o login do Windows ou a Autenticação do Servidor SQL. No caso do modo não misto, é necessário fazer login usando a Autenticação do Windows.

  Para modificar as configurações do modo de autenticação, no SQL Enterprise Manager, clique o botão direito do mouse no servidor cujas configurações devem ser modificadas (padrão: (local)(Windows NT)), selecione *propriedades*, clique na guia *Segurança* e selecione *Servidor SQL e Windows* ou *Apenas Windows* para Autenticação. A Conta de Serviço de Inicialização deve ser definida como *Conta do sistema*.

- Nome da Instância do Servidor SQL de Destino – (padrão recomendado).

  NOTA: Se você tiver especificado o nome da instância durante a instalação do Servidor SQL, use esse nome ao ser solicitado a fornecer o nome da instância do Servidor SQL ao instalar os componentes do Banco de Dados e/ou do DAS. Se não tiver especificado o nome da instância durante a instalação do Servidor SQL, deixe o nome da instância em branco durante a instalação (ou seja, se estiver digitando o nome de host, não adicione "\<nome_da_instância>" ao nome do host do banco de dados).

- Número de porta da Instância do Servidor SQL de Destino – (o padrão é 1433).
- Se for usar a Autenticação do Windows para um ou mais usuários do Sentinel, o usuário do domínio Windows correspondente precisa existir antes da instalação do Banco de Dados do Sentinel. Os usuários do Sentinel a seguir podem ser atribuídos a um usuário do domínio Windows:
  - Administrador do Banco de Dados do Sentinel – Proprietário do esquema do banco de dados (p. ex. – esecdba)
  - Usuário do Aplicativo Sentinel **-** Usado pelos aplicativos do Sentinel para a conexão com o banco de dados (p. ex. – esecapp)
  - Administrador do Sentinel – Administrador para fazer login no Sentinel Control Center (por exemplo, esecadm).
  - Usuário do Relatório do Sentinel – Usado para a criação de relatórios (p. ex. **-** esecrpt)

Sentinel Server

NOTA: Se o Banco de Dados do Sentinel não for instalado ao mesmo tempo em que o Sentinel Server, será necessário instalar o Banco de Dados do Sentinel primeiro.

Antes de instalar o Sentinel Server, será necessário:

- Para obter os requisitos de hardware, consulte os *Capítulos 1 e 2*
- Servidor Windows 2000 com Service Patch 4 ou Servidor Windows 2003 com Service Patch 1
- Número de série e Chave de licença do Sentinel 5 (Para DAS). Para obter mais informações, consulte Obtendo uma Chave de Licença.
- Se estiver instalando o DAS e usando uma conta de usuário de domínio Windows para o usuário do Aplicativo Sentinel, será necessário conceder a esse usuário o privilégio de 'Fazer Login como serviço'. Para isso, abra o painel de controle 'Política de Segurança Local' na máquina em que o DAS será instalado (*Iniciar* > *Configurações* > *Painel de Controle* > *Ferramentas Administrativas* > *Política de Segurança Local*). Na janela Política de Segurança Local, vá até *Políticas Locais* > *Atribuição de Direitos do Usuário*. Abra a política *Fazer login como serviço* e adicione o usuário.

- Servidor SMTP – Necessário para o envio de e-mails do Sentinel.

Sentinel Control Center e Assistente

Antes de instalar o Sentinel Server, será necessário:

- Para saber quais são os requisitos de hardware, consulte os *Capítulos 1 e 2*
- Servidor Windows 2000 com Service Patch 4 ou Servidor Windows 2003 com Service Patch 1.

Advisor

Para instalar o Advisor, será necessário obter um ID e senha do Advisor com a Novell. O Download Direto da Internet usa a porta 443.

NOTA: Caso pretenda usar o Advisor para o Exploit Detection somente, não é necessário instalar o software Crystal Enterprise. Isso só é obrigatório se a intenção for executar Crystal Reports para Sentinel. Consulte o *Capítulo 10, Configuração do Consultor*, para obter mais informações.

Instalação do Sentinel 5 para MS SQL

O Sentinel 5 dá suporte a dois tipos de instalação. São elas:

- Simples – Opção de instalação da all-in-one. Serviços do Sentinel para Windows, Serviço do Coletor e Aplicativos com o Servidor MS SQL na mesma máquina. Dá suporte apenas à autenticação do Servidor SQL. O tipo de instalação se destina a fins demonstrativos apenas.
- Personalizado – Permite uma instalação totalmente distribuída.

NOTA: Por padrão, o instalador define que os seguintes grupos de arquivos NÃO devem crescer automaticamente: ESENTD, ESENTX, SENT_SMRYD e SENT_SMRYX. Fica definido o crescimento automático de todos os outros grupos de arquivos. O motivo para não permitir o crescimento automático das tabelas ESENTD, ESENTX, SENT_SMRYD e SENT_SMRYX é que elas contêm dados de eventos e dados resumidos de eventos. A utilização do espaço para eventos e resumos pode ser altamente dinâmica. Esses grupos de arquivos devem ser monitorados e estendidos de forma controlada, com base na configuração do sistema de arquivos e levando em consideração o equilíbrio de E/S e o backup e recuperação de bancos de dados.

O gerenciamento de partições SDM (arquivamento, descarte e adição de partições) deve ser programado de modo a manter os dados do evento em tamanho controlado.

Instalação Simples

Essa opção instala todos os componentes (inclusive o banco de dados) em uma única plataforma e somente dá suporte à autenticação do Servidor SQL. Se destina principalmente a fins demonstrativos. Não é recomendada para uso em teste ou produção.

NOTA: A instalação simples não oferece suporte à autenticação de senha do Gerenciador de Coletor.

Instalação Simples do Sentinel

1. Verifique se você coletou as informações, realizou as tarefas e atendeu aos requisitos especificados na seção Pré-instalação do Sentinel 5 para MS SQL em relação aos componentes que está instalando.
2. Insira o CD de instalação do Sentinel na unidade de CD-ROM.
3. Procure o CD e clique duas vezes em *setup.bat*.

NOTA: Não há suporte para a instalação no modo de console no Windows.

4. Clique na seta para baixo e selecione uma das seguintes opções de idioma:
   - Inglês
   - Francês
   - Alemão
   - Italiano
   - Português
   - Espanhol
5. Depois de ler a tela de boas-vindas, clique em *Avançar*.
6. Aceite o Contrato de Licença de Usuário Final e clique em *Avançar*.

7. Aceite o diretório de instalação padrão ou clique em *Procurar* para especificar o local da instalação. Clique em *Avançar*.

8. Selecione *Simples*. Clique em *Avançar*.

9. Digite as informações sobre a configuração.
   - Número de Série e Chave de Licença
   - Servidor SMTP (o nome DNS ou o endereço IP) – essa opção permite ao Sentinel enviar e-mails.
   - Email – digite um endereço de e-mail válido para o qual os e-mails de notificação do Advisor devem ser enviados (p.ex. - Sent_Server@myserver.com).
   - Senha Global do Sistema – digite uma senha e a senha de confirmação correspondente. Esta será a senha de todos os usuários padrão. Isso inclui o usuário do sistema operacional esecadm e os usuários dos bancos de dados. Consulte o Banco de Dados do Sentinel, na seção Pré-instalação do Sentinel 5 para MSSQL, para obter a lista de usuários padrão do banco de dados criada durante a instalação.
   - Diretório de Dados – o local de todos os arquivos de dados do Banco de Dados e do Advisor. Para mudar o local padrão, clique no botão ... e selecione um local. O padrão é %ESEC_HOME%\data.

NOTA: Se estiver instalando o Advisor, a opção de instalação Simples irá configurar o Advisor para que use o Download Direto da Internet com um intervalo de atualização de 12 horas e todas as notificações de e-mail habilitadas.

   - Para instalar o Advisor, selecione *Instalar Consultor*. Digite um nome de usuário e senha. Se o nome de usuário ou senha não puder ser verificado, após clicar em *Avançar* você será perguntado se deseja continuar (não recomendado). Se optar por continuar, digite a senha do Advisor novamente na janela de confirmação de senha. Caso contrário, corrija a senha do Advisor.

Clique em *Avançar*.

Número de Série: | Chave de Licença:

Servidor SMTP: localhost | E-mail: esecadm

Senha Global do Sistema (usada para todos os usuários do Sentinel e o Gerenciador de Coletor)

Senha: | Confirmar Senha:

Diretório de Dados: C:\Archivos de programa\sentinel5.1.3.0\data ...

Instalar Consultor (digite o nome de usuário/senha abaixo)

Nome de Usuário: | Senha:

10. Para a configuração da instalação do banco de dados, digite:
    - Nome de usuário e senha do sa.
    - Se você especificou o nome da instância do Servidor SQL, digite esse nome.

Database Installation Configuration

SQL Server Instance:

Database Name: ESEC

Login: sa

Password:

11. Leia as informações apresentadas nas telas que aparecerem e clique em *Avançar* ao concluir. Depois de concluída a instalação, será necessário reinicializar o sistema.

NOTA: Caso deseje instalar algum software de Integração de Terceiros (Suporte técnico HP ou Integração do Remedy), após a reinicialização da máquina, execute o instalador novamente e selecione o software de Integração de Terceiros a ser instalado. Para obter mais informações, consulte o *Guia de Integração de Terceiros*.

Instalação Personalizada

Instalação Personalizada do Sentinel

1. Verifique se você coletou as informações, realizou as tarefas e atendeu aos requisitos especificados na seção Pré-instalação do Sentinel 5 para MS SQL em relação aos componentes que está instalando.
2. Insira o CD de instalação do Sentinel na unidade de CD-ROM.
3. Procure o CD e clique duas vezes em setup.bat.

NOTA: Não há suporte para a instalação no modo de console no Windows.

4. Clique na seta para baixo e selecione uma das seguintes opções de idioma:
   - Inglês
   - Francês
   - Alemão
   - Italiano
   - Português
   - Espanhol
5. Depois de ler a tela de boas-vindas, clique em *Avançar*.
6. Aceite o Contrato de Licença de Usuário Final e clique em *Avançar*.
7. Aceite o diretório de instalação padrão ou clique em *Procurar* para especificar o local da instalação. Clique em *Avançar*.

8. Selecione *Personalizado* (padrão). Clique em *Avançar*.
9. Selecione os recursos a serem instalados.

NOTA: Para obter mais informações sobre os componentes que podem ser instalados e em que locais para diferentes configurações, consulte o *Capítulo 1, Requisitos do Sistema*.

Os componentes a seguir podem ser instalados:

- Banco de Dados – instala o Banco de Dados do Sentinel.
- Servidor de Comunicação – instala o barramento de mensagens (iSCALE)
- Advisor
- Mecanismo de Correlação
- DAS
- Serviço do Coletor
- Construtor de Coletores
- Sentinel Control Center
- Gerenciador de Dados do Sentinel
- HP OpenView Service Desk
- Integração do Remedy

NOTA: Para obter informações sobre a instalação do HP OpenView Service Desk ou da Integração do Remedy, consulte o *Guia de Integração de Terceiros*.

NOTA: Se nenhum dos recursos filhos de *Serviços do Sentinel* for selecionado, anule a seleção do recurso *Serviços do Sentinel* também. Ele ficará esmaecido com uma marca de seleção se ainda estiver selecionado, mas todos os recursos filhos serão desmarcados.

NOTA: Como parte da instalação do componente Banco de Dados de Sentinel, o instalador irá colocar arquivos na pasta %ESEC_HOME%\utilities\db.

Banco de Dados
Serviços do Sentinel
Servidor de Comunicação
Consultor (a Instalação requer Senha e ID do Consultor)
Correlação
DAS
Sentinel Collector Service
Aplicativos
Construtor de Coletor do Sentinel
Centro de Controle do Sentinel
Gerenciador de Dados do Sentinel

10. Se você selecionou a instalação do DAS, será solicitado a fornecer:
    - Número de Série
    - Chave de Licença
11. Se você selecionou a instalação de qualquer componente de integração de terceiros, será solicitado a fornecer uma senha para desbloquear o(s) componente(s) de integração de terceiros selecionados. Para obter mais informações, consulte o *Guia de Integração de Terceiros.*
12. Se optou por instalar o Sentinel Control Center, aparecerá um prompt de tamanho de heap JVM (Java Virtual Machine):
    - Tamanho de heap JVM (MB) - Por padrão, é definido como metade do tamanho da memória física detectada na máquina, com um máximo de 1024 MB.
      Esse será o tamanho de heap JVM máximo usado somente pelo Sentinel Control Center.

Sentinel Control Center Configuration

The installer has detected 1047 MB of physical memory. Please specify the desired JVM heap size for Sentinel Control Center. The legal range is 64-1024.

JVM Heap Size (MB)

523

13. Se você optar por instalar o Serviço do Coletor, escolha proteger ou não proteger o Gerenciador do Coletor do Assistente com uma senha. Se você optar por proteger o Gerenciador do Coletor do Assistente, será solicitado a criar uma senha para ele.

NOTA: Para a proteção do Coletor com uma senha, será necessário digitar essa senha ao fazer o upload, download ou depuração de Coletores nesse Gerenciador do Coletor. Essa senha complementa o nome de usuário e senha do Sentinel necessários para fazer o login no Construtor de Coletor.

NOTA: Para obedecer as rígidas configurações de segurança exigidas pela Certificação de Critérios Comuns, o Sentinel exige uma senha forte com as seguintes características:

1. Escolha senhas com no mínimo 8 caracteres, que incluam ao menos um dígito em MAIÚSCULA, um em minúscula, um símbolo especial (!@#$%^&*()_+), e um dígito numérico (0-9).

2. A senha não pode conter o nome usado no e-mail nem partes do nome completo.

3. A senha não deve ser uma palavra "comum" (por exemplo, não deve ser uma palavra registrada em dicionário nem gíria de uso comum).

4. A senha não deve conter palavras de idioma algum, pois existem vários programas de invasão de senha capazes de verificar milhões de possibilidades de combinações de palavras em segundos.

5. Escolha uma senha de que possa se lembrar, mas que seja complexa. Por exemplo, Mft5#AIdade (Meu filho tem 5 anos de idade) OU EmnCh5#a (Eu moro na Califórnia há 5 anos).

14. Se optar por instalar o DAS, selecione a quantidade de RAM do sistema que deseja alocar para o Serviço de Acesso a Dados. No caso de ambientes distribuídos, recomenda-se selecionar o máximo de memória (4 GB). No caso de ambientes independentes, recomenda-se selecionar metade da memória RAM.

15. Para a instalação do banco de dados, será solicitado o seguinte:
    a. Selecione a plataforma do servidor do banco de dados de destino como Servidor Microsoft SQL 2000 ou 2005 e selecione uma das ações a seguir:
        - Criar um novo banco de dados com objetos de banco de dados – cria um novo banco de dados do MS SQL e preenche o novo banco com objetos de banco de dados.

- Adicionar objetos de banco de dados a um banco de dados vazio existente – somente adiciona um banco de dados a um banco de dados do MS SQL existente. O banco de dados existente precisa estar vazio.

b. Digite o diretório de registro de instalação do banco de dados (padrão: %ESEC_HOME%\logs\db). Aceite o 'Diretório do registro de instalação do banco de dados' padrão ou clique em *Procurar* para especificar um local diferente.

Selecione a plataforma do servidor do banco de dados de destino:

Microsoft SQL Server 2000

Criar um novo banco de dados com objetos de banco de dados.

Adicionar objetos de banco de dados a um banco de dados vazio existente.

Diretório do registro de instalação do banco de dados:

C:\Programme\sentinel5.1.3.0\logs\db

Procurar

c. Digite as informações sobre a configuração do Servidor SQL da seguinte maneira:

- (1) Nome de host ou endereço IP do banco de dados – por padrão, a máquina do host local será exibida, se o Servidor SQL estiver instalado localmente. Se o Servidor SQL que você deseja instalar não aparecer na lista suspensa, selecione *Outro* na lista. Será exibida uma caixa de texto permitindo que você digite o nome do host. O nome do host que você digitar deve ser totalmente qualificado (por exemplo, 'sqlserver.sentinel.net' em vez de apenas 'sqlserver'). Se tiver especificado um nome de instância durante a instalação do Servidor SQL, será preciso adicionar '\<nome_da_instância>' ao final do nome do host, em que <nome_da_instância> é o nome dado à instância durante a instalação do Servidor SQL.
- (2) Nome do Banco de Dados (Novo banco) – O nome a ser dado ao novo banco de dados do Servidor SQL. Além do banco de dados indicado aqui, outro banco de dados com o nome <seu_nome_bd>_WF também será criado para uso pelo iTRAC.
- (2) Nome do banco de dados (Banco existente) – O nome do banco de dados do Servidor SQL vazio ao qual deseja adicionar objetos de banco de dados. Use o nome do banco de dados que não contém o sufixo "_WF".
- (3) A porta do banco de dados (o padrão é 1433).
- Para o administrador do banco de dados do sistema, selecione:

  (4) Autenticação do Windows - irá usar o nome de usuário com o qual você estiver executando o instalador.

  (5) Autenticação do Servidor SQL - digite a senha do usuário sa.

Autenticação do Windows

Autenticação do Servidor SQL

d. Se você optou por instalar um novo banco de dados, digite o local dos arquivos de banco de dados a seguir:

NOTA: Para fins de recuperação e desempenho, recomenda-se que esses locais estejam em dispositivos de E/S diferentes.

- Arquivos de dados
- Arquivos de índice
- Arquivos de dados de resumo
- Arquivos de índice de resumo
- Arquivos de registro

e. Se você optou por instalar um novo banco de dados, digite o tamanho do banco:

- Padrão (20.000 MB) – capacidade para 30 dias com 500.000 eventos por dia
- Grande (400.000 MB) – capacidade para 30 dias com 10.000.000 eventos por dia
- Personalizado (especifique manualmente o tamanho). Se escolher essa opção, deverá fornecer também:
  (1) o tamanho do banco de dados em MB (de 10.000 a 2.000.000)
  (2) o tamanho de cada arquivo de registro em MB (de 100 a 100.000)
  (3) o tamanho máximo de cada arquivo de banco de dados em MB
  (de 2.000 a 100.000)

Please select Standard, Large, or Custom database size.

Standard (20,000MB, 30 day capacity @ 500,000 events per day)

Large (400,000MB, 30 day capacity @ 10,000,000 events per day)

Custom (specify database sizing manually)

f. Para o Administrador do Banco de Dados do Sentinel (DBA), selecione:

- Autenticação do Windows e digite <nome_do_domínio>\<nome_do_usuário>
- Autenticação do Servidor SQL (esecdba), a senha e a confirmação da senha, ou

---

NOTA: Se você selecionar *Autenticação do Servidor SQL*, não poderá modificar o nome de login padrão.

Digite as informações de autenticação do usuário do Administrador do Banco de Dados do Sentinel (DBA).

Autenticação do Windows

Autenticação do Servidor SQL

Login:

Autenticação do Windows

Digite as informações de autenticação do usuário do Administrador do Banco de Dados do Sentinel (DBA).

Autenticação do Windows

Autenticação do Servidor SQL

Login: esecdba

Palavra-passe:

Confirmar Senha:

Autenticação do Servidor SQL

g. Para o usuário do Banco de Dados do Aplicativo Sentinel, selecione:

NOTA: Se estiver usando um login do domínio Windows para o usuário do Banco de Dados do Aplicativo Sentinel, será necessário conceder a esse usuário o privilégio *Fazer login como Serviço* nessa máquina conforme especificado na seção Sentinel Server, dentro da seção Pré-instalação do Sentinel 5 para MS SQL.

- Autenticação do Windows, digite <nome_do_domínio>\<nome_do_usuário>, a senha e a confirmação da senha
- Autenticação do Servidor SQL (esecapp), digite a senha e a confirmação da senha

NOTA: Se você selecionar *Autenticação do Servidor SQL*, não poderá modificar o nome de login padrão.

Digite as informações de autenticação do usuário do Banco de Dados de Aplicativo do Sentinel.

Autenticação do Windows

Autenticação do Servidor SQL

Login:

Palavra-passe:

Confirmar Senha:

Autenticação do Windows

Digite as informações de autenticação do usuário do Banco de Dados de Aplicativo do Sentinel.

Autenticação do Windows

Autenticação do Servidor SQL

Login: esecapp

Palavra-passe:

Confirmar Senha:

Autenticação do Servidor SQL

h. Para o usuário Administrador do Sentinel, selecione:

- Autenticação do Windows e digite <nome_do_domínio>\<nome_do_usuário>
- Autenticação SQL, digite o nome de usuário do Administrador do Sentinel (padrão: esecadm), a senha e a confirmação da senha

NOTA: Se você selecionar *Autenticação do Servidor SQL*, não poderá modificar o nome de login padrão.

Digite as informações de autenticação do usuário do Administrador do Sentinel.

Autenticação do Windows

Autenticação do Servidor SQL

Login:

Autenticação do Windows

Digite as informações de autenticação do usuário do Administrador do Sentinel.

Autenticação do Windows

Autenticação do Servidor SQL

Login: esecadm

Palavra-passe:

Confirmar Senha:

Autenticação do Servidor SQL

i. Para o usuário de Relatórios do Sentinel, selecione:
   - Autenticação do Windows e digite <nome_do_domínio>\<nome_do_usuário>
   - Autenticação SQL (esecrpt), digite a senha e a confirmação da senha

---

NOTA: Se você selecionar *Autenticação do Servidor SQL*, não poderá modificar o nome de login padrão.

Digite as informações de autenticação do usuário do Administrador do Sentinel.

Autenticação do Windows

Autenticação do Servidor SQL

Login:

Autenticação do Windows

Digite as informações de autenticação do usuário do Sentinel Report.

Autenticação do Windows

Autenticação do Servidor SQL

Login: esecrpt

Palavra-passe:

Confirmar Senha:

Autenticação do Servidor SQL

j. Clique em *Avançar* na janela de resumo da instalação do banco de dados.

16. Se você optou por instalar o DAS, mas não optou por instalar o Banco de Dados do Sentinel, será solicitado a fornecer as informações do Banco de dados do Sentinel para o Servidor SQL a seguir. Essas informações serão usadas para configurar o DAS para que aponte para o Banco de Dados do Sentinel.

    - Nome de host ou endereço IP do banco de dados – por padrão, a máquina do host local será exibida, se o Servidor SQL estiver instalado localmente. Se o Banco de Dados do Sentinel para Servidor SQL que você deseja configurar para se conectar ao DAS não aparecer na lista suspensa, selecione *Outro* na lista. Será exibida uma caixa de texto permitindo que você digite o nome do host. O nome do host que você digitar deve ser totalmente qualificado (por exemplo, 'sqlserver.sentinel.net' em vez de apenas 'sqlserver'). Se tiver especificado um nome de instância durante a instalação do Servidor SQL, será preciso adicionar '\<nome_da_instância>' ao final do nome do host, em que <nome_da_instância> é o nome dado à instância durante a instalação do Servidor SQL.
    - Nome do banco de dados – O nome do Banco de Dados existente do Sentinel para Servidor SQL para o qual deseja configurar o DAS para se conectar. Use o nome do banco de dados que não contém o sufixo "_WF".
    - Porta do banco de dados (o padrão é 1433).
    - Para o usuário do Banco de Dados do Aplicativo Sentinel, selecione:

NOTA: Se estiver usando um login do domínio Windows para o usuário do Banco de Dados do Aplicativo Sentinel, será necessário conceder a esse usuário o privilégio "Fazer login como Serviço" nessa máquina conforme especificado na seção Sentinel Server, dentro da seção Pré-instalação do Sentinel 5 para MS SQL.

        - Autenticação do Windows - Especifique o login do domínio Windows dado para esse usuário durante a instalação do Banco de Dados do Sentinel e digite a senha para esse usuário. A senha é necessária nesse caso para configurar o Sentinel Windows Service como "Fazer login como Serviço" como esse login do domínio Windows.
        - Autenticação do Servidor SQL – Especifique o login "esecapp" e digite a senha dada para esse usuário durante a instalação do Banco de Dados do Sentinel.

Autenticação do Windows

Autenticação de SQL

17. Se você optou por instalar o DAS, configure o suporte de e-mail do Sentinel. Especifique o servidor SMTP e o endereço de e-mail do remetente a ser usado pelo Serviço de Execução para enviar mensagens (opcional – você pode editar isso manualmente após instalar [%ESEC_HOME%\sentinel\config\execution.properties]):

18. Se você optou por instalar o Advisor, aparecerá o prompt a seguir solicitando o tipo de instalação:
    - Download Direto da Internet – A máquina do Advisor está diretamente conectada à Internet. Nessa configuração, é feito o download automático das atualizações da Novell da Internet com regularidade.

- Independente – O Advisor é configurado como um sistema isolado que requer intervenção manual para receber uma atualização do Sentinel.

Please select the type of Advisor Installation

Direct Internet Download

StandAlone

19. Se você optou por instalar o Advisor e selecionou o uso do Download Direto da Internet, digite seu nome de usuário, senha e freqüência de atualização dos dados do Advisor. Se o nome de usuário ou senha não puder ser verificado, após clicar em *Avançar* você será perguntado se deseja continuar (não recomendado). Se optar por continuar, digite a senha do Advisor novamente na janela de confirmação de senha. Caso contrário, corrija a senha do Advisor.

Please enter the username and password to access the Advisor server and feed data:

Username:

Password:

Please select how often Advisor data needs to be updated:

6 Hours   12 Hours

20. Se você optou por instalar o Advisor, digite:
    - O diretório onde serão armazenados os arquivos de alimentação de dados do Advisor. Esse é o local onde serão gravados os arquivos de alimentação de ataque e alerta quando for feito seu download.
    - Endereço do destinatário para o envio de notificações por e-mail
    - Selecione Sim ou Não para o recebimento de e-mails sobre atualizações bem sucedidas do Advisor. As notificações de erro serão sempre enviadas.

Please enter the directory where Advisor data feed files are to be stored:

Browse

Enter the from address for sending the email notifications: Advisor

Enter the addresses to which email notifications should be sent (comma separated): esecadm

Do you want email notifications for successful Advisor updates (error notifications will always be sent)?

Yes   No

NOTA: Após a instalação, para mudar os endereços de e-mail do Advisor, edite os arquivos attackcontainer.xml e alertcontainer.xml. Para obter mais informações, consulte o *Capítulo 9 – Guia Consultor do Guia do Usuário do Sentinel*.

21. Se você optou por instalar o HP Service Desk ou a Integração do Remedy, será solicitado a fornecer informações adicionais. Para obter mais informações, consulte o *Guia de Integração de Terceiros do Sentinel*.

22. Leia as informações apresentadas nas telas que aparecerem e clique em *Avançar* ao concluir. Depois de concluída a instalação, será necessário reinicializar.
23. Clique em *Concluir* para reinicializar o sistema.
24. Se você espera uma taxa de eventos elevada (superior a 800 eventos por segundo), é necessário seguir as instruções de configuração adicionais contidas na seção Configurando a Estratégia de Inserção de Eventos dos Objetos de Dados Ativos (ADO).

Pós-instalação do Sentinel 5 para MS SQL

Atualizando o e-mail do Sentinel para autenticação SMTP

Se o sistema exigir autenticação SMTP, você precisará atualizar o arquivo execution.properties. Esse arquivo está na máquina em que o DAS foi instalado. Ele está localizado em %ESEC_HOME%\sentinel\config. Para configurar esse arquivo, execute mailconfig.bat para mudar o arquivo e mailconfigtest.bat para testar as mudanças.

Para configurar o arquivo execution.properties

1. Na máquina em que o DAS foi instalado, faça login como esecadm e mude para o diretório:

```
%ESEC_HOME%\sentinel\config
```

2. Execute mailconfig desta maneira:

```
mailconfig.bat -host <servidor SMTP> -from <endereço de
   e-mail de origem> -user <usuário de autenticação de
   e-mail> –password
```

Exemplo:

```
mailconfig.bat -host 10.0.1.14 -from meu_nome@domínio.com
   -user meu_nome_de_usuário –password
```

Depois de digitar esse comando, você será solicitado a fornecer uma nova senha.

```
Digite a senha:*********

Confirme a senha:*********
```

NOTA: Ao usar a opção password, ela deve ser o último argumento.

Para testar a configuração de execution.properties

1. Na máquina em que o DAS foi instalado, mude para o diretório:

```
%ESEC_HOME%\sentinel\config
```

2. Execute mailconfigtest desta maneira:

```
mailconfigtest.bat -to <endereço de e-mail de destino>
```

Se o e-mail for enviado com êxito, será exibida a seguinte mensagem na tela e o e-mail será recebido no endereço de destino.

```
O e-mail foi enviado com êxito!
```

Verifique a caixa de correio do e-mail de destino para confirmar o recebimento da mensagem. A linha de assunto e o conteúdo devem ser:

```
Assunto: Testando a propriedade de e-mail do Sentinel

Este é um teste da configuração da propriedade de e-mail
   do Sentinel. Se você vir esta mensagem, a propriedade
   de e-mail do Sentinel foi configurada corretamente
   para enviar e-mail
```

Banco de Dados do Sentinel

Após instalar o Banco de Dados do Sentinel, o banco irá conter os usuários padrão a seguir:

- esecdba – Proprietário do esquema (se estiver usando o usuário do domínio Windows, que pode ser configurado no momento da instalação).
- esecapp – Nome de usuário usado pelos aplicativos do Sentinel para a conexão com o banco de dados (se estiver usando o usuário do domínio Windows, que pode ser configurado no momento da instalação).
- esecadm – Administrador do Sentinel (se estiver usando o usuário do domínio Windows, que pode ser configurado no momento da instalação).
- esecrpt – Usuário de relatórios (se estiver usando o usuário do domínio Windows, que pode ser configurado no momento da instalação).

Serviço do Coletor

Durante a instalação do Serviço do Coletor, os seguintes Coletores serão instalados, cada qual com uma configuração de porta para sua execução.

Produto	Nome do Coletor
Coletores Demo	
Teste de upload de bens, funciona com o Coletor DemoEvents	DemoAssetUpload
Teste de eventos demo, funciona com o Coletor DemoAssetUpload e com o DemoVulnerabilityUpload	DemoEvents
Teste de upload de vulnerabilidade, funciona com o Coletor DemoEvents	DemoVulnerabilityUpload
Teste de envio de um evento	SendOneEvent
Teste de envio de vários eventos	SendMultipleEvents

NOTA: Para obter mais informações sobre a configuração dos Coletores Demo, consulte o *Capítulo 12 - Teste da Instalação*.

NOTA: Para ver Coletores adicionais, vá até o Sentinel Customer Portal. Para obter mais informações (inclusive sobre configuração) consulte a documentação que acompanha cada Coletor em:

%WORKBENCH_HOME%\Elements\<Nome do coletor>\Docs\

Para instalar Coletores adicionais, execute o script do Service Pack no CD do Service Pack. O script irá instalar os Coletores em nível local.

No Windows:

```
.\service_pack.bat
```

No UNIX:

```
./service_pack.sh
```

Para obter as instruções de instalação do Service Pack e uma lista de Coletores, consulte as *notas do Service Pack Release*.

Atualizando a Chave de Licença

Se a chave de licença do Sentinel expirou e a Novell emitiu uma nova, execute o programa da chave de software para atualizar a chave de licença.

Como atualizar a chave de licença

1. Faça login como um usuário com direitos administrativos.
2. Vá até %ESEC_HOME%\utilities.
3. Digite o seguinte comando:

   ```
   softwarekey.exe
   ```

4. Digite o número 1 como a chave principal. Pressione Enter.

Instruções de Configuração para o Uso da Autenticação do Windows para Servidor SQL com o Driver do DataDirect JDBC

NOTA: A que vem a seguir é extraído do Guia de Instalação do DataDirect Connect© para JDBC©. Recomenda-se enfaticamente que as seguintes ações sejam executadas pelo administrador do sistema.

Após a instalação do Connect para JDBC, é necessário configurar os componentes a seguir para usar a autenticação do Windows no Servidor SQL:

- Servidor de banco de dados do Servidor SQL
- Controlador de Domínio
- Estação de Trabalho Cliente

Para obter mais informações sobre a autenticação do Windows e o driver do Servidor SQL do Connect para JDBC, consulte o *Guia do Usuário e a Referência do DataDirect Connect para JDBC*.

Servidor de banco de dados do Servidor SQL

Esta seção descreve a configuração necessária no servidor de banco de dados do Servidor SQL para usar a autenticação do Windows com o driver do Servidor SQL do Connect para JDBC.

Nome do Princípio de Serviço

Para usar o protocolo de autenticação Kerberos, é necessário registrar um Nome de Princípio de Serviço (SPN) para cada instância de Servidor SQL. Um SPN é um nome exclusivo que mapeia o serviço do Servidor SQL de uma máquina e porta específicas para um nome de conta usado para iniciar o serviço (Conta de Inicialização de Serviço). Um SPN é composto pelos elementos a seguir:

- O nome da classe de serviço é sempre MSSQLSvc para o Servidor SQL
- O nome de host é o nome DNS completo da máquina que executa o Servidor SQL
- A porta é o número de porta em que a instância do Servidor SQL realiza a escuta.

Por exemplo: MSSQLSvc/DBServer.test:1433 é um SPN para uma instância do Servidor SQL em execução em uma máquina chamada DBServer no domínio de teste e fazendo escuta na porta 1433.

Listando SPNs

Verifique com o administrador de banco de dados ou domínio se os SPNs apropriados foram registrados para cada instância do Servidor SQL. O administrador de banco de dados ou domínio pode usar o comando do Windows ldifde para listar SPNs registrados.

Registrando SPNs

Se necessário, o administrador de banco de dados ou domínio pode registrar SPNs usando a ferramenta Setspn disponível com o Kit de Recursos do Windows. Por exemplo:

```
setspn -A MSSQLSvc/DBServer.test:1433 sqlsvc
```

Registra um SPN que mapeia a Conta de Inicialização de Serviço chamada sqlsvc para uma instância do Servidor SQL em execução em uma máquina chamada DBServer no domínio de teste e fazendo escuta na porta 1433.

A ferramenta Setspn está disponível no site na web a seguir: http://www.microsoft.com/windows2000/techinfo/reskit/tools/existing/setspn-o.asp.

Consulte a documentação da Microsoft que acompanha a ferramenta Setspn para obter instruções sobre seu uso.

NOTA: Se a Conta de Inicialização do Servidor SQL for mudada, será necessário apagar e repetir o registro dos SPNs para o Servidor SQL.

Modo de Autenticação

Para usar a autenticação do Windows, o modo de autenticação do Servidor SQL pode ser definido com um dos modos a seguir:

- Autenticação do Windows apenas
- Autenticação mista

Se a autenticação do Servidor SQL será usada além da autenticação do Windows, o modo de autenticação precisa ser definido para usar a autenticação Mista:

Controlador de Domínio

O driver do Servidor SQL dá suporte à autenticação do Windows quando o Centro de Distribuição de Chave (KDC) Kerberos está em execução em um controlador de domínio do Windows 2000. Ao se comunicar com o KDC, as mensagens que circulam entre o KDC e o Servidor SQL são criptografadas.

Como o Servidor SQL somente pode usar o algoritmo de criptografia DES-CBC-MD5, a Conta de Inicialização de Serviço do Servidor SQL no controlador de domínio precisa conter a propriedade de Diretório Ativo "Usar tipos de criptografia DES para esta conta." Verifique com o administrador de domínio se essa propriedade está definida para a Conta de Inicialização de Serviço do Servidor SQL. A Conta de Inicialização de Serviço do Servidor SQL não pode ser usada como a conta de login cliente.

Máquina Cliente

Esta seção descreve a configuração necessária na máquina cliente para usar a autenticação do Windows com o driver do Servidor SQL do Connect para JDBC.

Arquivo de Configuração Kerberos

O módulo de login Kerberos necessita do nome do domínio Kerberos (nome do domínio Windows) e do nome KDC (nome do controlador do domínio Windows) para esse domínio Kerberos. Quando o Connect para JDBC é instalado, um arquivo de configuração é instalado para especificar um domínio Kerberos genérico e um nome KDC. Esse arquivo recebe o nome de krb5.conf e é instalado no diretório /lib do diretório de instalação do Connect para JDBC.

Modifique o arquivo krb5.conf para especificar o nome do domínio Kerberos e o nome KDC para o ambiente. Se o arquivo não for modificado para incluir um domínio Kerberos válido e um nome KDC, o erro a seguir é gerado:

```
Mensagem:[DataDirect][Driver do JDBC do Servidor SQL]Não
      foi possível estabelecer uma conexão usando a
      segurança integrada: Nenhuma credencial válida
      fornecida
```

O driver do Servidor SQL do Connect para JDBC automaticamente configura o módulo de login Kerberos para carregar o arquivo de configuração do Kerberos krb5.conf, a menos que a propriedade do sistema java.security.krb5.conf já esteja definida para apontar para outro arquivo de configuração. Para anular o nome do domínio Kerberos e o nome KDC especificados no arquivo krb5.conf, especifique as propriedades do sistema a seguir: java.security.krb5.realm e java.security.krb5.kdc.

Configurando a Estratégia de Inserção de Eventos dos Objetos de Dados Ativos (ADO)

O Sentinel 5.1 oferece uma estrutura para a inclusão de diferentes estratégias para a inserção de eventos no banco de dados. O Sentinel 5.1 oferece duas estratégias para a inserção de eventos no banco de dados do MS SQL:

- JDBCLoadStrategy
- ADOLoadStrategy

A estratégia a ser usada para a inserção de eventos é regida pela propriedade da estratégia de inserção do componente EventStoreService do arquivo das_binary.xml.

A estratégia JDBC é a estratégia padrão configurada out of the box.

A estratégia ADO é uma estratégia de inserção nativa para a agilização da inserção de eventos. Essa estratégia requer que os pacotes do Windows adicionais sejam instalados na máquina que está executando o componente DAS. Consulte a seção abaixo para obter informações sobre os pacotes que precisam ser instalados. A estratégia ADO precisa ser usada em configurações para as quais é esperada uma alta taxa de eventos.

O número de eventos a ser agrupado para inserção no banco de dados é regido pela propriedade insert.batchsize. Essa propriedade insert.batchsize é usada por todas as estratégias de inserção de eventos.

As seções abaixo descrevem como migrar para as estratégias de carga de ADO.

Pré-requisitos para a ADOLoadStrategy

O conector nativo ADO precisa da estrutura .net e do pacote J# redistribuível a ser instalado na máquina que estiver executando o Binário DAS.

NOTA: Será necessário desinstalar versões antigas da estrutura .net e do pacote J# redistribuível para instalar as versões listadas na ordem a seguir.

- estrutura net 2.0 Beta 2 disponível em http://www.microsoft.com/downloads/details.aspx?FamilyID=7ABD8C8F-287E-4C7E-9A4A-A4ECFF40FC8E&displaylang=en
- visual J# versão 2.0 Beta 2 disponível em http://www.microsoft.com/downloads/details.aspx?FamilyId=A2788A92-76AB-4BF4-893A-FA9FD5031F14&displaylang=en

Configurando a Estratégia de Inserção de Eventos de Carga de ADO

Para mudar a estratégia de inserção de eventos do Sentinel da Estratégia de Inserção JDBC padrão para a Estratégia de Inserção ADO, há algumas etapas que precisam ser executadas.

Mudando da Estratégia de Inserção JDB para a Estratégia de Inserção ADO.

1. Usando um editor de texto, abra %ESEC_HOME%\sentinel\config\das_binary.xml.
2. Faça uma pesquisa no texto a seguir:

```
JDBCLoadStrategy
```

3. Mude esse texto para:

   ```
   ADOLoadStrategy
   ```

4. Grave esse mudança no arquivo das_binary.xml.
5. Reinicie o aplicativo binário DAS.

Após a reinicialização do Binário DAS, os arquivos %ESEC_HOME%\Sun-1.4.2\bin\EventInsert.dll e EventJNICLIBridge.dll serão carregados e usados para realizar as inserções de eventos no banco de dados via ADO.

Dicas de Depuração de ADO

A interface ADO somente registrará mensagens de erro no arquivo %ESEC_HOME%\sentinel\log\ADOEventStoreError.log. As mensagens de erro iniciais gravadas no arquivo de registro podem incluir mensagens de falha de conexão ao banco de dados. Esse arquivo também registrará exceções que ocorrem durante a inserção de eventos no banco de dados. Nota: somente erros são registrados nesse arquivo,

Para verificar se o ADO foi conectado e carregado corretamente verifique o arquivo de registro das_binary localizado no diretório %ESEC_HOME%\sentinel\log.

A interface ADO também registra erros no arquivo das_binary localizado no diretório %ESEC_HOME%\sentinel/log. Os erros registrados no arquivo de registro das_binary log incluem falhas na localização/carregamento da biblioteca EventJNICLIBridge.dll, falhas de conexão ao banco de dados e falhas de inserção de Associações de Eventos/Evento.

Se mensagens de erro indicarem que conectores nativos não foram carregados corretamente, verifique o seguinte:

- Verifique se a máquina possui a versão certa da estrutura .net e do pacote J# redistribuível instaladas.
- Verifique se os arquivos "EventJNICLIBridge.dll" e "EventInsert.dll" estão localizados no diretório %ESEC_HOME%\Sun-1.4.2\bin\.

6 Migração de dados e patch para o Oracle no Solaris

NOTA: O termo Agente é sinônimo de Coletor. De agora em diante, Agentes serão referidos como Coletores.

Este capítulo aborda:

- Migração de dados e atualização da v4.2.0 até a v5.1.3
- Patch v5.x.x até a v5.1.3

Migração de dados e upgrade da v4.2 até a v5.1.3

O processo de upgrade do Sentinel 5 com Migração de Dados da v4.2.0 consiste em:

- Pré-migração
  - Faça backup da instância do Banco de Dados do Sentinel: isso permitirá restaurar o banco de dados v4.2 caso ocorram falhas inesperadas.
  - Faça o backup de qualquer script ou comando do sistema do menu popup que possa estar no diretório $ESEC_HOME.
  - Exporte as regras de correlação do Sentinel v4.2 (se houver). Consulte Pré-migração – Exportando regras de correlação para obter instruções.
  - Faça backup de scripts de coletores e configurações de porta. Consulte Pré-migração – Fazendo backup de scripts de coletores e configuração de porta para obter instruções.
  - Com exceção do componente Banco de Dados, desinstale o Sentinel v4.2. Consulte Pré-migração – Desinstalando a v4.2 para obter instruções.
  - Instale somente o banco de dados do Sentinel 5. Consulte Pré-migração – Instalando o banco de dados do Sentinel 5 para obter instruções.
- Migração
  - Execute o utilitário de migração de dados. Consulte Migração para obter instruções.
- Pós-migração
  - Instale os outros componentes do Sentinel 5. Consulte Pós-migração – Instalando o Sentinel 5 para obter instruções.
  - Instale o Service Pack mais recente do Sentinel.
  - Inicie o Sentinel 5.
  - Importe as regras de correlação (se houver). Consulte Pós-migração – Instalando o Sentinel 5 para obter instruções.
  - Copie os scripts do coletor e as configurações de porta do local do backup para o local de instalação do Sentinel 5. Consulte Pós-migração – Reconfigurando scripts de coletor e configurações de porta para obter instruções.
  - Redefina as configurações do Oracle 9i Cliente relacionado ao Crystal Reporting para que aponte para o banco de dados do Sentinel 5 e importe os Gabaritos de Crystal Report do Sentinel 5. Consulte Pós-migração – Configurando o Sentinel 5 para o Crystal Reporting para obter instruções.

Sentinel Server

O Sentinel 5 requer que a versão anterior do software seja desinstalada antes de incluir os componentes do Sentinel 5 Server. Não desinstale a versão anterior (v4.2) do Banco de Dados pois ela é necessária para fazer a migração dos dados da v4.2 para o Sentinel 5. Faça backup da máquina do Sentinel Server (diretório de instalação $ESEC_HOME e unidade Root) antes de desinstalar. Isso permitirá restaurar a v4.2 caso ocorram falhas inesperadas.

As seções a seguir fornecem instruções detalhadas sobre a migração de dados e a pré e a pós-instalação.

Gerenciador de Coletores

O Sentinel 5 requer que todos os Gerenciadores de Coletor da v4.2 sejam desinstalados antes da instalação do software do Gerenciador de Coletor do Sentinel 5. Faça backup da máquina do Gerenciador de Coletor da v4.2 (diretório de instalação $ESEC_HOME e unidade Root) antes de desinstalar.

Para cada máquina que executa o Gerenciador de Coletor v4.2 com no mínimo uma porta configurada, você deve gravar uma cópia do conteúdo destes diretórios em um local de fácil acesso. O conteúdo desses diretórios será usado durante a pós-migração para reconfigurar rapidamente as portas de Coletores na instalação da v4.2:

- $WORKBENCH_HOME/Agents – Contém os arquivos de configuração de porta.
- $WORKBENCH_HOME/Elements – Contém os scripts do Coletor.
- Se você não fizer uma cópia do conteúdo dos diretórios acima, precisará reconfigurar todos os scripts do Coletor e as portas.

NOTA: O Gerenciador de Coletor v4.2 e o Construtor de Coletor não são compatíveis com os componentes da v5.

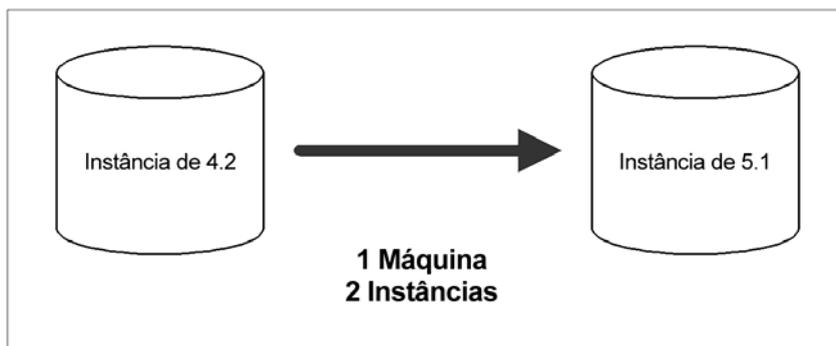
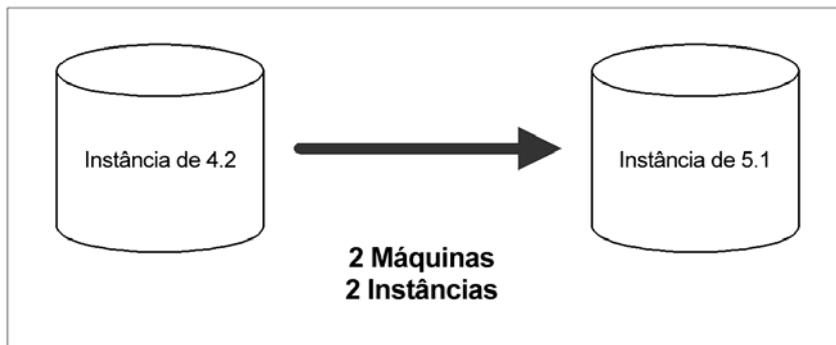
As seções a seguir fornecem instruções detalhadas sobre a migração de dados e a pré e a pós-instalação.

Crystal Reporting Server

Você deve usar os relatórios mais recentes do Service Pack mais atual depois de fazer o upgrade para o Sentinel 5. Os novos relatórios foram desenvolvidos para funcionarem com o novo esquema de banco de dados. Para obter o Service Pack mais recente, entre em contato com o Suporte Técnico da Novell.

Servidor do banco de dados

É fornecido um utilitário de migração de dados do Sentinel 5 para copiar dados de um banco de dados do Sentinel 4.2.0 no Solaris 8/9 para um banco de dados do Sentinel v5.1.2 no Solaris 9. O utilitário de migração de dados oferece suporte em:

- 1 máquina com 2 instâncias de bancos de dados

- 2 máquinas com 1 instância de banco de dados em cada máquina.

A migração dos dados a seguir é feita pelo utilitário:

- Usuários e permissões designadas
- Filtros
- Opções de configuração do menu popup.
- Tags CV renomeadas
- Configurações de arquivo e partição
- Os casos da v4.2 são copiados na v5 como incidentes
- Incidentes e eventos relacionados a incidentes

NOTA: O utilitário de migração de dados NÃO migrará dados de eventos, exceto quando os dados do evento estiverem associados a incidentes. Só será feita a migração dos dados de evento associados a incidentes.

NOTA: Os dados de evento de incidente não podem ser vistos no Sentinel Control Center. Esses dados podem ser exibidos usando o Crystal Reporting ou consultas ao SQL.

As seções a seguir fornecem instruções detalhadas sobre a migração de dados e a pré e a pós-instalação.

Pré-migração – Exportando regras de correlação

Exportando um conjunto de regras de correlação

1. No Console do Sentinel v4.2, na guia Admin, abra a janela Regras de Correlação.
2. Selecione um conjunto de regras.
3. Clique em *Exportar*. Na janela de explorador de arquivos que se abre, procure o dispositivo de destino no qual gravar a regra e clique em *OK*. O conjunto de regras será exportado como um arquivo xml.

Pré-migração – Fazendo backup de scripts de coletores e configuração de porta

Fazendo backup de scripts de coletores e configuração de porta

1. Em todas as máquinas Sentinel v4.2 que executam o Gerenciador de Coletor, crie um diretório para armazenar todos os scripts de coletores e configurações de porta para essa máquina.

2. No diretório recém-criado, crie um arquivo de texto listando o nome de todos os coletores que estão sendo usados por uma configuração de porta nesse Gerenciador de Coletor. Use um Construtor de Coletor para determinar os coletores usados por esse Gerenciador de Coletor. Se esse Gerenciador de Coletor estiver no Solaris, será preciso usar um Construtor de Coletor em uma máquina Windows (não há suporte para o Construtor de Coletor no Solaris).
3. Copie estes diretórios no diretório recém-criado:
   - $WORKBENCH_HOME/Agents
   - $WORKBENCH_HOME/Elements

Pré-migração – Desinstalando a v4.2

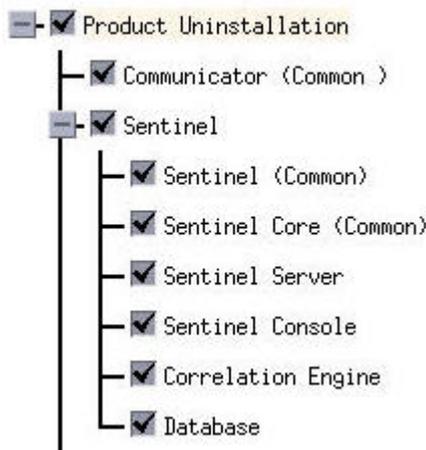
Desinstalando a v4.2

1. Na máquina que contém o Sentinel v4.2 e em máquinas cliente, feche todos os Consoles do Sentinel e Construtores de Coletores.
2. Faça login como usuário Root.
3. Pare o Sentinel Server.
4. Use o comando cd para:

```
$ESEC_HOME/_uninst
```

5. Digite:

```
./uninstall.bin
```

6. Siga os prompts na tela. Selecione os aplicativos para desinstalação. Selecione todos os recursos.

NOTA: Se tiver um software de terceiros, selecione-o para desinstalá-lo.

7. Clique nos prompts da tela até que seja exibida a janela Desinstalação do Banco de Dados.
8. Na janela Desinstalação do Banco de Dados, selecione *Não apagar nada*.

Do you want to delete the database?

- Delete the entire database instance.
- Delete only the database objects.
- Delete nothing.

9. Clique para fechar as janelas de desinstalação restantes.
10. Reinicialize o sistema.

Pré-migração - instalando o banco de dados do Sentinel 5

Instalação do banco de dados do Sentinel 5

1. Verifique se você coletou as informações, executou as tarefas e preencheu os requisitos especificados na seção Banco de Dados do Sentinel, no *Capítulo 3*: Instalando o Sentinel 5 para o *Oracle* - *Pré-instalação do Sentinel 5 para o Oracle*.
2. Para verificar a Configuração do Oracle revisando a seção Configuração do Oracle no *Capítulo 3*: *Instalando o Sentinel 5 para o Oracle* - *Pré-instalação do Sentinel 5 para o Oracle*.
3. Faça login como usuário Root.
4. Insira e monte o CD de instalação do Sentinel.
5. No CD, localize o diretório completo.
6. Para iniciar o programa de instalação, vá para o diretório de instalação no CD-ROM e digite:

   Para o modo de interface gráfica:

   ```
   ./setup.sh
   ```

   ou

   Para modo textual:

   ```
   ./setup.sh –console
   ```

7. Depois de ler a tela de boas-vindas, clique em *Avançar*.
8. Aceite o Contrato de Licença de Usuário Final e clique em *Avançar*.
9. Aceite o diretório de instalação padrão ou clique em *Procurar* para especificar o local da instalação. Clique em *Avançar*.

   Nome do directório:

   /opt/sentinel5.1.3.0

   Procurar

10. Selecione *Personalizado* (padrão). Clique em *Avançar*.
11. Nos recursos a serem instalados, desmarque todos os recursos e selecione *Apenas Banco de Dados*. Clique em *Avançar*.

   NOTA: Verifique se desmarcou o recurso pai *Serviços do Sentinel*. Ele ficará esmaecido com uma marca de seleção se ainda estiver selecionado, mas todos os recursos filho serão desmarcados.

12. Especifique o nome de usuário do Administrador do Sentinel no sistema operacional e o local do diretório pessoal. Esse é o nome de usuário que terá a propriedade do produto Sentinel instalado. Se o usuário não existir ainda, um usuário será criado com um diretório pessoal no diretório especificado.
    - Nome de usuário do Administrador do sistema operacional – O padrão é esecadm
    - Diretório pessoal do Administrador do sistema operacional – O padrão é "/export/home". Se o nome de usuário for esecadm, o diretório pessoal do usuário será /export/home/esecadm.

NOTA: Se um novo usuário for criado, sua senha precisará ser definida manualmente, separadamente desse instalador. Recomenda-se enfaticamente que isso seja feito diretamente pelo registro no sistema após a instalação do produto.

NOTA: Para obedecer as rígidas configurações de segurança exigidas pela Certificação de Critérios Comuns, o Sentinel exige uma senha forte com as seguintes características:

1. Escolha senhas com no mínimo 8 caracteres, que incluam ao menos um dígito em MAIÚSCULA, um em minúscula, um símbolo especial (#$_) e um dígito numérico (0-9). Não use espaços.

2. A senha não pode conter o nome usado no e-mail nem partes do nome completo.

3. A senha não deve ser uma palavra "comum" (por exemplo, não deve ser uma palavra registrada em dicionário nem gíria de uso comum).

4. A senha não deve conter palavras de idioma algum, pois existem vários programas de invasão de senha capazes de verificar milhões de possibilidades de combinações de palavras em segundos.

5. Escolha uma senha de que possa se lembrar, mas que seja complexa. Por exemplo, Mft5#AIdade (Meu filho tem 5 anos de idade) OU EmnCh5#a (Eu moro na Califórnia há 5 anos).

13. Digite o nome do host (ou o IP) e o número da porta (padrão: 10012) do Servidor de Comunicação. Clique em *Avançar*.
14. Selecione a plataforma do servidor do banco de dados de destino como Oracle e selecione uma das ações a seguir:
    - Criar um novo banco de dados com objetos de banco de dados – cria uma nova instância de banco de dados Oracle e preenche a nova instância com objetos de banco de dados.
    - Adicionar objetos de banco de dados a um banco de dados vazio existente – somente adiciona um banco de dados a uma instância de banco de dados Oracle existente. A instância de banco de dados Oracle existente precisa estar vazia, exceto pela presença do usuário esecdba.
15. Digite o diretório de registro de instalação do banco de dados (padrão: $ESEC_HOME/logs/db). Aceite o 'Diretório do registro de instalação do banco de dados' padrão ou clique em Procurar para especificar um local diferente.

16. Clique em *OK* no nome de usuário do Oracle padrão.

17. Se você optou por criar um novo banco de dados, digite o seguinte:
    - O caminho para o arquivo de driver do Oracle JDBC (o nome típico do arquivo .jar é ojdbc14.jar). Esse é o caminho completo para o arquivo .jar, normalmente $ORACLE_HOME/jdbc/lib/ojdbc14.jar (não é possível usar variáveis de ambiente nesse campo).
    - Nome de host – O nome de host da máquina onde o banco de dados será instalado. Esse campo não é configurável se uma nova instância de banco de dados estiver sendo criada.
    - Nome do Banco de Dados – O nome da instância de banco de dados que será instalada.

NOTA: Você precisará dar ao banco de dados um nome diferente daquele especificado na instalação da versão 4.2.

---

18. Se você optou por adicionar objetos de bancos de dados a um banco Oracle vazio existente, será solicitado a fornecer as informações a seguir.

   - O caminho para o arquivo de driver do Oracle JDBC (o nome típico do arquivo .jar é ojdbc14.jar). Esse é o caminho completo para o arquivo .jar, normalmente $ORACLE_HOME/jdbc/lib/ojdbc14.jar (não é possível usar variáveis de ambiente nesse campo).
   - Nome de host do banco de dados ou endereço IP – O nome ou endereço IP do host onde está o banco de dados Oracle ao qual você deseja adicionar objetos de banco de dados. Pode ser o nome de host local ou um nome de host remoto.
   - Nome do banco de dados – O nome da instância do banco de dados Oracle vazio existente à qual você deseja adicionar objetos de banco de dados (o padrão é ESEC. Você precisará dar ao banco de dados um nome diferente daquele especificado na instalação da versão 4.2). Esse nome de banco de dados precisa aparecer como nome de um serviço no arquivo tnsnames.ora (no diretório $ORACLE_HOME/network/admin/) da máquina onde o instalador está sendo executado.

NOTA: Se o nome do banco de dados não estiver no arquivo tnsnames.ora, o instalador não exibirá um erro nesse momento da instalação (porque ele verifica a conexão usando uma conexão JDBC direta), mas a instalação do Banco de dados irá falhar quando o instalador tentar se conectar ao banco de dados por meio de sqlplus. Se a instalação do banco de dados falhar nesse ponto, modifique o nome do serviço desse banco de dados no arquivo tnsnames.ora nessa máquina, sem sair do instalador, retroceda uma tela no instalador e avance novamente. Será feita uma nova tentativa de instalação do banco de dados com os novos valores no arquivo tnsnames.ora.

   - Porta do banco de dados (o padrão é 1521).
   - Para o usuário Administrador do Banco de Dados do Sentinel (DBA), especifique a senha do usuário *esecdba*. A senha do esecdba precisa coincidir com a senha da instalação da v4.2) O campo de nome de usuário desse prompt não é editável.

19. Se você optou por criar um novo banco de dados, verá o prompt a seguir:
    - Memória Oracle (MB) – A quantidade de memória RAM a ser alocada a essa instância de banco de dados Oracle.
    - Porta de Escuta – a porta onde criar uma escuta Oracle (o padrão é 1521).
    - Senha e confirmação de senha do usuário SYS – SYS é um usuário do Oracle padrão que será criado na nova instância de banco de dados. A senha desse usuário será definida como o valor especificado aqui.
    - Senha e confirmação de senha do usuário SYSTEM – SYSTEM é um usuário do Oracle padrão que será criado na nova instância de banco de dados. A senha desse usuário será definida como o valor especificado aqui.

20. Se você optar por criar um novo banco de dados, será solicitado a digitar o tamanho do banco: Você tem as opções a seguir:
    - Padrão (20 GB)
    - Grande (400 GB)
    - Personalizado (especifique manualmente o tamanho). Se você escolher essa opção, será solicitado a fornecer:
        - o tamanho inicial de cada arquivo de banco de dados em MB (100 a 10.000)
        - o tamanho máximo de cada arquivo de banco de dados em MB (2.000 a 100.000)
        - o tamanho de todos os arquivos de banco de dados em MB (7.000 a 2.000.000)

- o tamanho de cada arquivo de registro em MB (100 a 100.000)

Please select Standard, Large, or Custom database size.

Standard (20,000MB, 30 day capacity @ 500,000 events per day)

Large (400,000MB, 30 day capacity @ 10,000,000 events per day)

Custom (specify database sizing manually)

21. Se você optar por criar um novo banco de dados, será solicitado a digitar o local de armazenamento dos arquivos de bancos de dados a seguir:

NOTA: Para fins de recuperação e desempenho, recomenda-se que esses locais estejam em dispositivos de E/S diferentes.

Como o instalador não irá criar esses diretórios, eles precisam ser criados externamente antes de avançar.

Esses diretórios precisam permitir gravação pelo usuário do Oracle. Para tornar esses diretórios graváveis pelo usuário do Oracle, execute os comandos a seguir para cada diretório como Usuário Root:

```
chown –R oracle:dba <directory_path>
chmod –R 770 <directory_path>
```

supondo que "oracle" é seu nome de usuário no Oracle e que "dba" e seu nome de grupo no Oracle.

- Diretório de dados
- Diretório de índices
- Diretório de Dados de Resumo
- Diretório de Índices de Resumo
- Diretório Temporário e Desfazer Tabela:
- Diretório A do Membro de Redo Log
- Diretório B do Membro de Redo Log

22. Se você optou por criar um novo banco de dados, digite as informações de autenticação do Administrador do Banco de Dados do Sentinel (DBA). Este é o esecdba, o proprietário dos objetos de banco de dados.
23. Digite as informações de autenticação do usuário do banco de dados do aplicativo Sentinel. Este é o esecapp, o nome do usuário do aplicativo Sentinel que os processos do Sentinel usam para a conexão com o banco de dados.

24. Digite as informações de autenticação do usuário do Banco de Dados do Administrador do Sentinel. Este é o esecadm, o usuário Administrador do Sentinel.
25. Clique em *Avançar* na janela de resumo da instalação do banco de dados.
26. Depois de concluída a instalação, será necessário reinicializar. Clique em *Concluir* para reinicializar o sistema.

Migração

O utilitário de migração de dados migra apenas os seguintes itens:

- Usuários e permissões designadas.
- Filtros
- Opções de configuração do menu popup.
- Tags CV renomeadas
- Configurações de arquivo e partição
- Os casos da v4.2 são copiados na v5 como incidentes
- Incidentes e eventos relacionados a incidentes

NOTA: O utilitário de migração de dados NÃO migrará dados de eventos, exceto quando os dados do evento estiverem associados a incidentes. Só será feita a migração dos dados de evento associados a incidentes.

NOTA: Os dados de evento de incidente não podem ser vistos no Sentinel Control Center. Esses dados podem ser exibidos usando o Crystal Reporting ou consultas ao SQL.

Para os bancos de dados do Sentinel 4.2 que não estejam usando esecdba como o Proprietário do Esquema de Bancos de Dados do Sentinel

NOTA: Esse procedimento adicionará o ID para o banco de dados v4.2 permita a migração da v4.2 até a v5.

1. Para o Solaris, faça o login como o proprietário do software Oracle.
2. Use o comando cd para:

```
$ESEC_HOME/utilities/db/scripts/ddl/oracle/Migration
```

3. Usando o SQL*Plus, conecte-se ao banco de dados v4.2 como SYSDBA.
4. No prompt do SQL (SQL>), digite:

```
@import_add_esecdba.sql
```

5. Saia doSQL*Plus.

NOTA: Depois de executar a migração dos dados, é possível usar o Oracle Enterprise Manager para pagar o usuário esecdba do banco de dados do Sentinel 4.2.

Migração de dados

NOTA: No Solaris, o Utilitário de Migração de Dados usa o Oracle*Net para se conectar ao banco de dados do Sentinel 5 e entre os bancos de dados do Sentinel 5 e 4.2. Verifique se o arquivo tnsnames.ora onde o utilitário de migração de dados está sendo executado contém entradas do banco de dados do Sentinel 4.2 e 5 para que as conexões do Oracle*Net podem ser estabelecidas.

1. Faça login como usuário Root.
2. Verifique as variáveis de ambiente para garantir que o java (versão 1.4.2) está na variável PATH. Para realizar essa verificação, execute este comando na linha de comando:

```
java -version
```

   Se esse comando não tiver êxito, localize onde o java foi instalado no sistema ou faça o download e instale o java. Em seguida, atualize a variável de ambiente PATH para incluir o executável do java. Por exemplo, se o java estiver instalado no diretório:

```
/opt/sentinel5.1.3.0/Sun-1.4.2
```

   Adicione o seguinte no início da variável de ambiente PATH:

```
/opt/sentinel5.1.3.0/Sun-1.4.2/bin:
```

3. Monte o CD de instalação do software Sentinel 5 no servidor de banco de dados onde reside o banco de dados do Sentinel 5.
4. Use o comando cd para mudar para o diretório a seguir dentro do CD de instalação do software Sentinel 5:

```
sentinel/dbsetup/bin
```

5. Execute o comando:

```
./MigrateDb.sh
```

6. Você será solicitado a fornecer o seguinte:
   - O nome do host do banco de dados (no qual o banco de dados do Sentinel 5 está migrando).
   - O nome do banco de dados de destino (do banco de dados do Sentinel 5 para o qual está migrando)
   - A senha do esecdba (que deve ser idêntica à do usuário esecdba nos bancos de dados do Sentinel v4.2 e v5)
   - O nome do banco de dados de origem (nome do banco de dados v4.2)
   - O diretório de registro (no qual os arquivos de registro da migração de dados serão colocados)
   - A opção de migração:
     - (1) Configurações do sistema
     - (2) Incidentes/casos
     - (3) Ambos
     - (4) Nenhum

NOTA: A migração das configurações do sistema deve ser executada com êxito para poder migrar incidentes e casos.

NOTA: Se houver falha na migração das configurações do sistema, desinstale o banco de dados do Sentinel 5 selecionando a opção "Apagar apenas os objetos de banco de dados". Em seguida, reinstale o banco de dados do Sentinel 5 com a opção "Adicionar objetos de banco de dados a um banco de dados vazio existente".
Por último, repita as instruções da migração de dados.

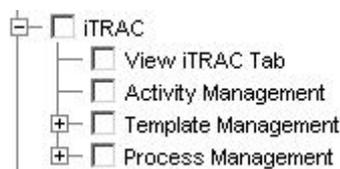
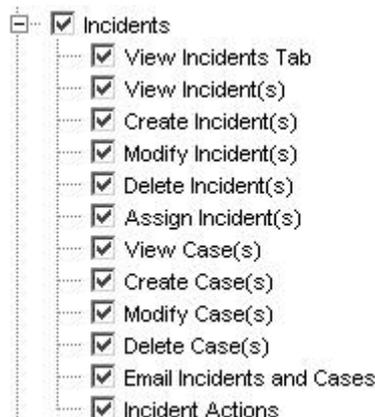
NOTA: Se houver falha da migração de incidentes, execute-a novamente. O utilitário de migração será reiniciado no ponto da falha. Não será necessário executar tarefas adicionais de limpeza.

NOTA: Depois de executar a migração dos dados, você pode usar o Oracle Enterprise Manager para apagar o usuário esecdba do banco de dados do Sentinel 4.2, caso tenha sido necessário adicioná-lo ao Utilitário de Migração de Dados.

Pós-migração - Instalando o Sentinel 5

No Sentinel 5, os seguintes recursos são novos, diferentes ou foram removidos.

- iTRAC – Esta é uma funcionalidade nova. As permissões de usuário associadas são:

iTRAC
View iTRAC Tab
Activity Management
Template Management
Process Management

- Incidentes – foi adicionada a Administração de Incidentes. Todas as funcionalidades relacionadas a casos foram removidas. As permissões de usuário associadas são:

Incidentes do Sentinel v4.2 | **Incidentes do Sentinel v5**

- Gerenciamento de Coletor – na v4.2 chamava-se Monitoramento de Assistente. 'Guia Exibir Assistentes' mudou para 'Exibir Coletores'. 'Controlar Assistentes e Coletor' mudou para 'Controlar Coletores' e 'Administração do Coletor'. As permissões de usuário associadas são:

Wizard Monitoring
View Wizards Tab
Control Wizards and Agents

Monitoramento de Assistente do Sentinel v4.2

Collector Management
View Collectors
Control Collectors
Collector Administration

Gerenciamento de Coletor do Sentinel v5

- Administração – adição de Estatísticas do DAS, Gerenciamento de Sessão de Usuário e Gerenciamento de Função do iTRAC. 'Regras de Correlação' foi renomeado para 'Correlação'. O recurso Configuração de Evento foi movido para o Gerenciador de Dados do Sentinel. 'Configuração do Usuário' foi renomeado como 'Gerenciamento do Usuário'. As permissões de usuário associadas são:

Administração do Sentinel v4.2 **Administração do Sentinel v5**

- ActiveViews™ - na v4.2, chamava-se Tempo Real. 'Exibições de Resumo' foi renomeado como Active Views. As permissões de usuário associadas são:

Tempo Real do Sentinel v4.2 **Active Views™ do Sentinel v5**

- A funcionalidade Visão Geral do Sistema não está disponível no Sentinel 5.

Instalando o Sentinel 5

1. Instale o Sentinel 5, consulte o capítulo sobre instalação 'Instalando o Sentinel para o Oracle'.
2. Instale o Service Pack mais recente do Sentinel.
3. Execute as etapas a seguir se quiser adicionar novas funcionalidades para os usuários existentes da v4.2:
   a. Verifique se o Sentinel Server está em execução.
   b. Faça login no Sentinel Control Center como usuário com permissão de Administração/Gerenciamento de Usuário (por exemplo, esecadm).
   c. No Sentinel Control Center, clique na guia Admin. Expanda Configuração do Usuário no painel Navegação ou, na barra de navegação, clique em *Admin > Configuração do Usuário*.
   d. Clique o botão direito do mouse no usuário ao qual deseja adicionar a funcionalidade (por exemplo, esecadm) e selecione *Detalhes do Usuário*. Clique na guia *Permissões*.
   e. Expanda iTRAC e atribua as permissões de acordo com a necessidade.
   f. Expanda Incidentes e atribua 'Administração de Incidentes', de acordo com a necessidade.

g. Expanda Gerenciamento de Coletor e atribua 'Administração do Coletor' conforme o necessário.
    h. Expanda Administração e atribua 'Estatísticas do DAS', 'Gerenciamento de Sessão de Usuário' ou 'Gerenciamento de Função do iTRAC' conforme o necessário.
    i. Clique na guia *Funções* e atribua a Função de Workflow Admin ou Analista, conforme o necessário.
    j. Clique em *OK*.

4. Se aplicável, importe as regras de correlação. Os conjuntos de regras exportados do Sentinel 4.2 aparecerão como pastas de regras quando importados para o Sentinel 5.
5. Copie do backup os scripts de Coletor e configurações de porta seguindo as instruções na seção Pós-migração – Reconfigurando scripts de coletor e configurações de porta

Pós-migração – reconfigurando scripts de coletor e configurações de porta

Em cada máquina na qual o Sentinel 5 Collector Service (Gerenciador de Coletor) estiver instalado, execute as etapas a seguir para restabelecer os scripts de coletor e as configurações de porta que foram usados na instalação do Sentinel v4.2.

Para restabelecer os scripts de coletor e as configurações de porta

1. Para parar o Gerenciador de Coletor, execute o comando a seguir como usuário esecadm:

```
$ESEC_HOME/wizard/agent-manager.sh parar
```

2. No local em que você colocou um backup do diretório $WORKBENCH_HOME/Agents da instalação do Sentinel v4.2, copie os seguintes arquivos para o diretório $WORKBENCH_HOME/Agentes da instalação atual do Sentinel 5 (sobregrave os arquivos, se necessário):
    - localhost_portcfg.dat
    - localhost_snmpcfg.dat
3. Leia o arquivo de texto criado durante a Pré-migração que lista todos os coletores usados pela instalação do Gerenciador de Coletor do Sentinel v4.2 nesta máquina. Você precisará saber os nomes de coletor para executar a próxima etapa.
4. No local em que você colocou um backup do diretório $WORKBENCH_HOME/Elements da instalação do Sentinel v4.2, copie os diretórios cujos nomes correspondem aos nomes no arquivo de texto no diretório $WORKBENCH_HOME/Elements da instalação atual do Sentinel 5 (sobregrave os arquivos e diretórios, se necessário).
5. Obtenha o utilitário UpgradePortCfgFile no site de Suporte Técnico do Sentinel (faça o download aqui).
6. Extraia o arquivo ZIP UpgradePortCfgFile.
7. Abra um prompt de comando e mude os diretórios no diretório do utilitário UpgradePortCfgFile extraído. Nesse diretório, execute o comando:

```
./UpgradePortCfgFile.sh
```

8. Execute o comando a seguir como Usuário Root para garantir a correta definição da propriedade dos arquivos recém-copiados:

```
chown –R esecadm:esec $ESEC_HOME/wizard
```

9. Para iniciar o Gerenciador de Coletor, execute o comando a seguir como usuário esecadm:

```
$ESEC_HOME/wizard/agent-manager.sh iniciar
```

Pós-migração – Configurando o Sentinel 5 para o Crystal Reporting

Se você estiver executando o Crystal Reporting para Sentinel 4.2 e quiser executar o Crystal Reporting com o Sentinel 5, será preciso:

- Modificar as configurações do Oracle 9i Cliente relacionado ao Crystal Reporting para apontarem para o banco de dados do Sentinel.
- Importar os gabaritos do Crystal Report (incluindo os gabaritos de migração de dados) do Service Pack mais recente.

Consulte o capítulo sobre instalação 'Crystal Reports' para obter mais informações.

Patch da v5.x.x até a v5.1.3

Execute este procedimento em qualquer máquina que tenha componentes do Sentinel instalados.

Se estiver executando o instalador de patches na máquina em que o componente Banco de Dados foi instalado originalmente, você precisará saber a senha do usuário administrador do banco de dados do Sentinel (esecdba).

Fazendo upgrade da v5.x.x até a v5.1.3 para o Solaris

1. Faça login como usuário Root.
2. Se aplicável, faça uma cópia de backup do arquivo syslog.conf.

NOTA: Se você estiver executando a v5.1.1sp1 ou superior e fez alterações no arquivo syslog.conf, será necessário fazer uma cópia do arquivo syslog.conf.
O instalador de patch sobregravará o arquivo syslog.conf. Após aplicar o patch, modifique ou sobregrave o novo arquivo syslog.conf para corresponder ao arquivo syslog.conf. original.

3. Insira e monte o CD de patch do Sentinel.
4. Para iniciar o programa de instalação, vá para o diretório de patch apropriado no CD-ROM e execute o comando:

   Para o modo de interface gráfica:

```
./setup.sh
```

   ou

   Para modo textual:

```
./setup.sh –console
```

5. Na tela de boas-vindas, clique em *Avançar*.

6. Aceite o Contrato de Licença de Usuário Final e clique em *Avançar*.
7. Clique em *Avançar* até chegar à janela de informações do banco de dados.
8. Verifique se o tipo do banco de dados está correto. Selecione o local do diretório do registro de instalação do banco de dados. Clique em *Avançar*.
9. Verifique se as informações do servidor Oracle estão corretas. Digite a senha do esecdba. Siga os outros prompts do instalador.

Atualizando o conector syslog

Se estiver usando os scripts do conector syslog de uma versão anterior do Sentinel para 5.1.1.1 (ou seja - 5.0, 5.0.1.0, 5.1.0.0, ou 5.1.1.0) você deve iniciar usando os scripts do conector de syslog que está incluído no patch. Para alternar o uso do script do conector syslog antigo para os scripts do conector syslog novo, remova o script antigo e instale o novo script.

O conector syslog é instalado com scripts que são executados no Windows e UNIX com arquivos de configuração aprimorados. Além disso, a instalação do servidor proxy syslog como um serviço foi simplificada.

Para remover o conector syslog

1. Efetue login como Usuário Root.
2. cd $ESEC_HOME/wizard/syslog
3. ./syslog-server.sh remove

Para instalar o conector syslog

1. Efetue login como Usuário Root.
2. cd $ESEC_HOME/wizard/syslog
3. ./syslog-server.sh install
4. Se você fez alterações no arquivo syslog.conf da instalação original, será necessário modificar ou sobregravar o novo arquivo syslog.conf para refletir o arquivo syslog.conf original. Ele está localizado em:

```
$ESEC_HOME/wizard/syslog/config
```

Atualização adicional para a v5.0.x até a v5.1.3

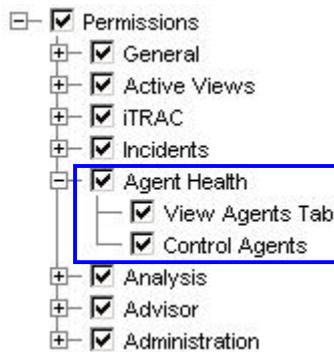
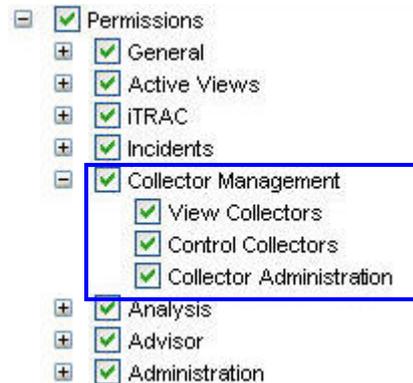
Após aplicar o patch da v5.0.x para a v5.1.3, é necessário atualizar as opções Permissões de Gerenciamento de Usuário e Configuração de Menu. Opcionalmente, você pode atualizar a permissão Telas de Servidor.

Atualizando as Permissões de Gerenciamento do Usuário para a v5.0.x até a v5.1.3

Durante o upgrade da v5.0.x ou para a v5.1.3, a Saúde do Coletor é mudada para o Gerenciamento de Coletor com a inclusão de uma funcionalidade adicional de Administração de Coletor.

Atualizando as permissões de Gerenciamento do Usuário

1. Faça login no Sentinel Control Center como usuário com permissão de Administração/Gerenciamento de Usuário.

Na v5.1, a Saúde do Coletor em Permissões foi mudada de 'Saúde do Coletor' para 'Gerenciamento de Coletor' com a inclusão de uma permissão adicional.

Permissão de usuário do Sentinel v5.0

Permissão de usuário do Sentinel v5.1.x

2. No Sentinel Control Center, clique na guia Admin. Expanda Configuração do Usuário no painel Navegação ou, na barra de navegação, clique em *Admin* > *Configuração do Usuário*.
3. Clique o botão direito do mouse em um usuário Admin (ou seja, esecadm ou outro usuário admin) > *Detalhes do Usuário*. Clique na guia *Permissões*.
4. Expanda Gerenciamento de Coletor e atribua *Administração do Coletor*. Clique em *OK*.

Atualizando Opções de Configuração do Menu para a v5.0.x até a v5.1.3

Se entradas adicionais na Configuração do Menu tiverem sido criadas antes do upgrade para a v5.1, os caminhos aos comandos precisão ser atualizados. A partir da versão 5.1.0.0, no Solaris, o comando a ser executado na Configuração do Menu precisar existir no diretório $ESEC_HOME/sentinel/exec. Além disso, todos os caminhos aos comandos executados na Configuração do Menu são sempre relativos ao diretório $ESEC_HOME/sentinel/exec. Se você precisar executar um comando em outro local do sistema de arquivos, crie um link simbólico de um local em $ESEC_HOME/sentinel/exec para o comando em execução.

A Configuração de Menu para rota de rastreamento precisa ser mudada manualmente de 'tracert' para 'traceroute' para funcionar corretamente.

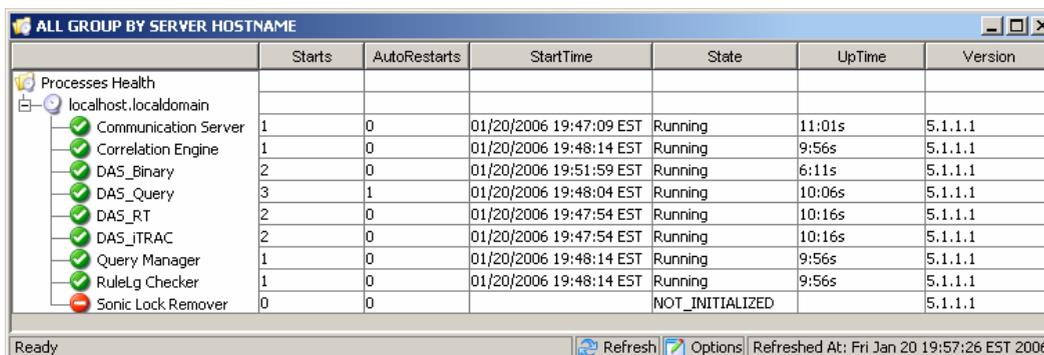
Para adicionar uma opção ao menu de Configuração do Menu

1. Faça login no Sentinel Control Center como usuário com permissão de Administração/Gerenciamento de Usuário.
2. Clique na guia *Admin*.
3. No Navegador de Admin, clique em *Admin* > *Configuração de Menu*.
4. Na janela Configuração do Menu, clique em *Modificar* e realce um item de menu que deva ser atualizado. Clique em *Detalhes*.
5. Na caixa de diálogo Configuração do Menu, faça as mudanças necessárias em:
   - Linha de comando/URL
   - Parâmetros – precisam vir dentro do sinal de porcentagem (e.g., %EventName%)

NOTA: Para obter uma lista dos tags disponíveis que você pode usar ao especificar parâmetros, clique em Ajuda na caixa de diálogo Configuração do Menu, ou vá até o capítulo Metatag no Guia de Referência do Usuário Sentinel.

6. Clique em *OK*.
7. Clique em *Gravar*.

Atualizando Opções de Telas de Servidor para a v5.0.x até a v5.1.3

Para usar a tela de servidor após a instalação do patch, é necessário conceder a permissão "Telas de Servidor" ao usuário do Sentinel que esteja usando o Gerenciador do Usuário. O Gerenciador do Usuário fica localizado sob a guia Admin do Sentinel Control Center.

	Starts	AutoRestarts	StartTime	State	UpTime	Version
Processes Health						
localhost.localdomain						
Communication Server	1	0	01/20/2006 19:47:09 EST	Running	11:01s	5.1.1.1
Correlation Engine	1	0	01/20/2006 19:48:14 EST	Running	9:56s	5.1.1.1
DAS_Binary	2	0	01/20/2006 19:51:59 EST	Running	6:11s	5.1.1.1
DAS_Query	3	1	01/20/2006 19:48:04 EST	Running	10:06s	5.1.1.1
DAS_RT	2	0	01/20/2006 19:47:54 EST	Running	10:16s	5.1.1.1
DAS_iTRAC	2	0	01/20/2006 19:47:54 EST	Running	10:16s	5.1.1.1
Query Manager	1	0	01/20/2006 19:48:14 EST	Running	9:56s	5.1.1.1
RuleLg Checker	1	0	01/20/2006 19:48:14 EST	Running	9:56s	5.1.1.1
Sonic Lock Remover	0	0		NOT_INITIALIZED		5.1.1.1

Crystal Reporting Server

Depois de fazer o upgrade para o Sentinel 5.1.3, incluindo a aplicação do Service Pack mais recente, você deve importar os relatórios do Service Pack mais atual. Para obter mais informações, consulte o capítulo sobre o *Crystal Reports*, no *Guia de Instalação do Sentinel*.

Atualizando o e-mail do Sentinel para autenticação SMTP

Se o sistema exigir autenticação SMTP, você precisará atualizar o arquivo execution.properties. Esse arquivo está na máquina em que o DAS foi instalado. Ele está localizado em $ESEC_HOME/sentinel/config. Para configurar esse arquivo, execute mailconfig.sh para mudar o arquivo e mailconfigtest.sh para testar as mudanças.

Para configurar o arquivo execution.properties

1. Na máquina em que o DAS foi instalado, faça login como esecadm e mude para o diretório:

```
$ESEC_HOME/sentinel/config
```

2. Execute mailconfig desta maneira:

```
./mailconfig.sh -host <servidor SMTP> -from <endereço
   de e-mail de origem> -user <usuário de autenticação
   de e-mail> –password
```

Exemplo:

```
./mailconfig.sh -host 192.0.2.14 -from
   meu_nome@domínio.com -user meu_nome_de_usuário –
   password
```

Depois de digitar esse comando, você será solicitado a fornecer uma nova senha.

```
Digite a senha:*********

Confirme a senha:*********
```

NOTA: Ao usar a opção password, ela deve ser o último argumento.

Para testar a configuração de execution.properties

1. Na máquina em que o DAS foi instalado, faça login como esecadm e mude para o diretório:

   ```
   $ESEC_HOME/sentinel/config
   ```

2. Execute mailconfigtest desta maneira:

   ```
   ./mailconfigtest.sh -to <endereço de e-mail de destino>
   ```

   Se o e-mail for enviado com êxito, será exibida a seguinte saída na tela e o e-mail será recebido no endereço de destino.

   ```
   O e-mail foi enviado com êxito!
   ```

   Verifique a caixa de correio do e-mail de destino para confirmar o recebimento da mensagem. A linha de assunto e o conteúdo devem ser:

   ```
   Assunto: Testando a propriedade de e-mail do Sentinel

   Este é um teste da configuração da propriedade de e-
      mail do Sentinel. Se você vir esta mensagem, a
      propriedade de e-mail do Sentinel foi configurada
      corretamente para enviar e-mail
   ```

7 Migração de dados e patch para MS SQL

NOTA: O termo Agente é sinônimo de Coletor. De agora em diante, Agentes serão referidos como Coletores.

Este capítulo discute a migração de dados e o upgrade para:

- Migração de dados e atualização da v4.2.1 até a v5.1.3.
- Patch da v5.x.x até a v5.1.3

Migração de dados e upgrade da v4.2 até a v5.1.3

O processo de upgrade do Sentinel 5 com Migração de Dados da v4.2.0 consiste em:

- Pré-migração
  - Faça o backup da instância do banco de dados do Sentinel Server: isso permitirá restaurar o banco de dados da v4.2 caso ocorram falhas inesperadas.
  - Faça o backup de qualquer script ou comando do sistema do menu popup que possa estar no diretório %ESEC_HOME%
  - Exporte as regras de correlação do Sentinel v4.2 (se houver). Consulte Pré-migração – exportando regras de correlação para obter instruções.
  - Faça backup de scripts de coletores e configurações de porta. Consulte Pré-migração – fazendo backup de scripts de coletores e configuração de porta para obter instruções.
  - Com exceção do componente Banco de Dados, desinstale o Sentinel v4.2. Consulte Pré-migração – desinstalando v4.2 para obter instruções.
  - Instale somente o banco de dados do Sentinel 5. Consulte Pré-migração – instalando o banco de dados do Sentinel 5 para obter instruções.
- Migração
  - Execute o utilitário de migração de dados. Consulte Migração para obter instruções.
- Pós-migração
  - Instale os outros componentes do Sentinel 5. Consulte Pós-migração – instalando o Sentinel 5 para obter instruções.
  - Instale o Service Pack mais recente do Sentinel.
  - Inicie o Sentinel 5.
  - Importe as regras de correlação (se houver). Consulte Pós-migração – instalando o Sentinel 5 para obter instruções.
  - Copie os scripts do coletor e as configurações de porta do local do backup para o local de instalação do Sentinel 5. Consulte Pós-migração – reconfigurando scripts de coletor e configurações de porta para obter instruções.
  - Se você estiver executando o Crystal Server com o Sentinel, importe os gabaritos do Crystal Report do Sentinel 5. Consulte Pós-migração – configurando o Sentinel 5 para usar Crystal Reports para obter instruções.

Sentinel Server

O Sentinel 5 requer que a versão anterior do software seja desinstalada antes de incluir os componentes do Sentinel 5 Server. Não desinstale a versão anterior (v4.2) do Banco de Dados, pois ela é necessária para fazer a migração dos dados da v4.2 para o Sentinel 5. Faça backup da máquina do Sentinel Server (diretório de instalação %ESEC_HOME% e unidade Root) antes de desinstalar. Isso permitirá restaurar a v4.2 caso ocorram falhas inesperadas.

As seções a seguir fornecem instruções detalhadas sobre a migração de dados e a pré e a pós-instalação.

Gerenciador de Coletores

O Sentinel 5 requer que todos os Gerenciadores de Coletor da v4.2 sejam desinstalados antes da instalação do software do Gerenciador de Coletor do Sentinel 5. Faça backup da máquina

do Gerenciador de Coletor da v4.2 (diretório de instalação %ESEC_HOME% e unidade Root) antes de desinstalar.

Para cada máquina que executa o Gerenciador de Coletor v4.2 com no mínimo uma porta configurada, você deve gravar uma cópia do conteúdo destes diretórios em um local de fácil acesso. O conteúdo desses diretórios será usado durante a pós-migração para reconfigurar rapidamente as portas de Coletores na instalação da v4.2:

- %WORKBENCH_HOME%/Agents – contém os arquivos de configuração de porta.
- %WORKBENCH_HOME%/Elements – contém os scripts do Coletor.
- Se você não fizer uma cópia do conteúdo dos diretórios acima, precisará reconfigurar todos os scripts do Coletor e as portas.

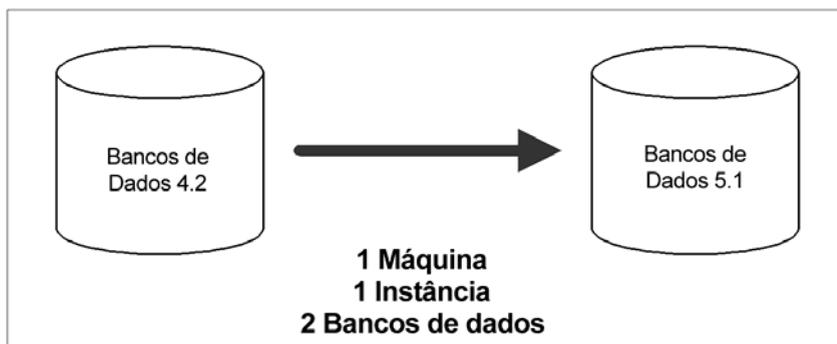
NOTA: O Gerenciador de Coletor v4.2 e o Construtor de Coletor não são compatíveis com os componentes da v5.

As seções a seguir fornecem instruções detalhadas sobre a migração de dados e a pré e a pós-instalação.

Crystal Reporting Server

Você deve usar os relatórios mais recentes do Service Pack mais atual depois de fazer o upgrade para o Sentinel 5. Os novos relatórios foram desenvolvidos para funcionarem com o novo esquema de banco de dados. Para obter o Service Pack mais recente, entre em contato com o Suporte Técnico do Sentinel.

Servidor do banco de dados

É fornecido um utilitário de migração de dados do Sentinel 5 para copiar dados do Sentinel 4.2.1 para o Sentinel v5.1.3. Esse utilitário só tem suporte para migração com o banco de dados do Sentinel 4.2.1 e do Sentinel 5.1.3 na mesma máquina e na mesma instância do SQL Server, mas cada um em um banco de dados diferente.

Os itens a seguir são migrados:

- Usuários e permissões designadas
- Filtros
- Opções de configuração do menu popup.
- Tags CV renomeadas
- Configurações de arquivo e partição
- Os casos da v4.2 são copiados na v5 como incidentes
- Incidentes e eventos relacionados a incidentes

NOTA: O utilitário de migração de dados NÃO migrará dados de eventos, exceto quando os dados do evento estiverem associados a incidentes. Só será feita a migração dos dados de evento associados a incidentes.

NOTA: Os dados de evento de incidente não podem ser vistos no Sentinel Control Center. Esses dados podem ser exibidos usando o Crystal Reporting ou consultas ao SQL.

Pré-migração – Exportando regras de correlação

Importando ou exportando um conjunto de regras de correlação

1. No Console do Sentinel v4.2, na guia Admin, abra a janela Regras de Correlação.
2. Selecione um conjunto de regras.
3. Clique em *Exportar*. Na janela de explorador de arquivos que se abre, procure o dispositivo de destino no qual gravar a regra e clique em *OK*. O conjunto de regras será exportado como um arquivo xml.

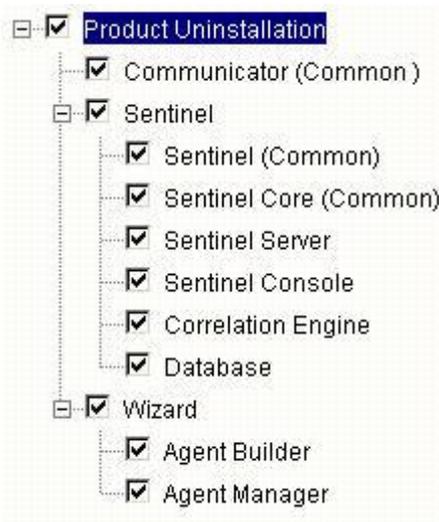
Pré-migração – Fazendo backup de scripts de coletores e configuração de porta

Fazendo backup de scripts de coletores e configuração de porta

1. Em todas as máquinas Sentinel v4.2 que executam o Gerenciador de Coletor, crie um diretório para armazenar todos os scripts de coletores e configurações de porta para essa máquina.
2. No diretório recém-criado, crie um arquivo de texto listando o nome de todos os coletores que estão sendo usados por uma configuração de porta nesse Gerenciador de Coletor. Use um Construtor de Coletor para determinar os coletores usados por esse Gerenciador de Coletor. Se o Gerenciador de Coletor estiver no UNIX, será preciso usar um Construtor de Coletor em uma máquina Windows (não há suporte para o Construtor de Coletor no UNIX).
3. Copie estes diretórios no diretório recém-criado:
   - %WORKBENCH_HOME%\Agents
   - %WORKBENCH_HOME%\Elements

Pré-migração – Desinstalando a v4.2

Desinstalando a v4.2

1. Na máquina Sentinel v4.2:
   - Feche todos os Consoles e Construtores de Coletor do Sentinel
   - Clique em *Iniciar* > *Programas* > *Sentinel* > *Desinstalar o Sentinel 4.2.1.x*.
2. Clique nos prompts da tela até que seja exibida a janela de desinstalação de recursos. Selecione todos os recursos.

NOTA: No exemplo acima, não está sendo mostrado nenhum software de integração de terceiros. Se tiver um software de terceiros, selecione-o para desinstalá-lo.

Clique nos prompts da tela até que seja exibida a janela Desinstalação do Banco de Dados.

3. Na janela Desinstalação do Banco de Dados, selecione *Não executar ação alguma no banco de dados*.

Please select which database uninstall action to perform:

Delete the entire database instance.

Delete only the database objects.

Perform no action on the database.

4. Clique para fechar as janelas de desinstalação restantes.

Pré-migração - instalando o banco de dados do Sentinel 5

Instalação do banco de dados do Sentinel 5

1. Verifique se a variável de ambiente não faz referência à versão 4.2. Se fizer, exclua a variável. Estas variáveis de ambiente não devem estar presentes:
   - ESEC_HOME
   - ESEC_VERSION
   - ESEC_JAVA_HOME
   - ESEC_CONF_FILE
   - WORKBENCH_HOME
2. Verifique se você coletou as informações, executou as tarefas e preencheu os requisitos especificados na seção Banco de Dados do Sentinel, no *Capítulo 4*: *Instalando o Sentinel 5 para MS SQL - Pré-instalação do Sentinel 5 para MS SQL*.
3. Insira o CD de instalação do Sentinel na unidade de CD-ROM.
4. Procure o CD e clique duas vezes em *setup.bat*.

NOTA: Não há suporte para a instalação no modo de console no Windows.

5. Clique na seta para baixo e selecione uma das seguintes opções de idioma:
   - Inglês
   - Francês
   - Alemão
   - Italiano
   - Português
   - Espanhol
6. Depois de ler a tela de boas-vindas, clique em *Avançar*.
7. Aceite o Contrato de Licença de Usuário Final e clique em *Avançar*.
8. Aceite o diretório de instalação padrão ou clique em *Procurar* para especificar um local diferente. Clique em *Avançar*.

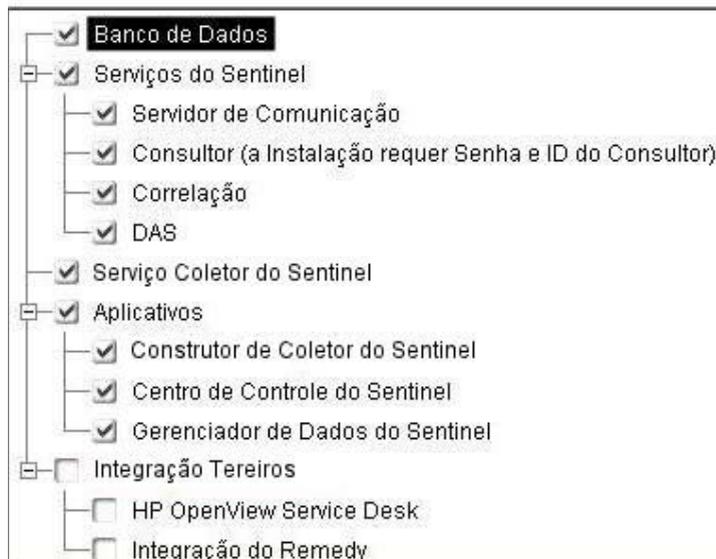
Faça clique em Seguinte para instalar "Sentinel 5" neste directório ou em Procurar para instalar num outro directório.

Nome do directório:

C:\Programme\sentinel5.1.3.0

Procurar

9. No tipo de instalação, selecione *Personalizado* (padrão). Clique em *Avançar*.
10. Nos recursos a serem instalados, desmarque todos os recursos e selecione *Apenas Banco de Dados*. Clique em *Avançar*.

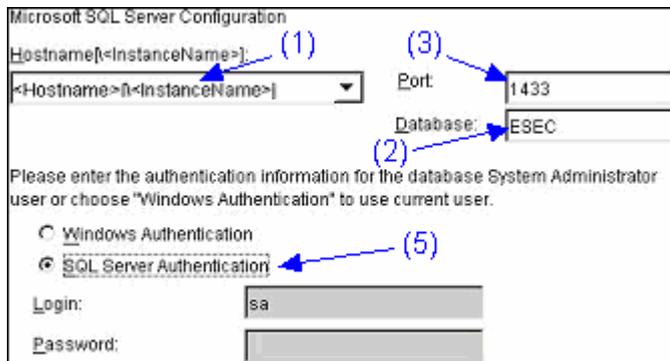
NOTA: Verifique se desmarcou o recurso pai "Serviços do Sentinel". Ele ficará esmaecido com uma marca de seleção se ainda estiver selecionado, mas todos os recursos filho serão desmarcados.

11. Digite o nome do host (ou o IP) e o número da porta (padrão: 10012) do Servidor de Comunicação. Clique em *Avançar*.
12. Selecione Microsoft SQL Server como a plataforma de banco de dados de destino e selecione *Criar um novo banco de dados com objetos de banco de dados*. Digite

também o diretório do registro de instalação do banco de dados (padrão: %ESEC_HOME%\logs\db). Aceite o *Diretório do registro de instalação do banco de dados* padrão ou clique em *Procurar* para especificar um local diferente. Clique em *Avançar*.

13. Digite as informações sobre a configuração do SQL Server:
    - (1) Nome de host ou endereço IP do banco de dados – por padrão, a máquina do host local será exibida, se o Servidor SQL estiver instalado localmente. Se o Servidor SQL que você deseja instalar não aparecer na lista suspensa, selecione *Outro* na lista. Será exibida uma caixa de texto permitindo que você digite o nome do host. O nome do host que você digitar deve ser totalmente qualificado (por exemplo, 'sqlserver.sentinel.net' em vez de apenas 'sqlserver'). Se tiver especificado um nome de instância durante a instalação do Servidor SQL, será preciso adicionar '\<nome_da_instância>' ao final do nome do host, em que <nome_da_instância> é o nome dado à instância durante a instalação do Servidor SQL.
    - (2) O nome que será dado ao novo banco de dados SQL Server. Além do banco de dados indicado aqui, outro banco de dados com o nome <seu_nome_bd>_WF também será criado para uso pelo iTRAC.

NOTA: Você precisará dar ao banco de dados um nome diferente daquele especificado na instalação da versão 4.2.

- (3) A porta do banco de dados (o padrão é 1433).
- Para o administrador do banco de dados do sistema, selecione:
    - (4) Autenticação do Windows (usará o nome de usuário com o qual você estiver executando o instalador) ou
    - (5) Autenticação do SQL Server. Digite a senha do usuário sa.

Autenticação do Windows

Autenticação do SQL Server

14. Digite o local destes arquivos de banco de dados:

NOTA: Para fins de recuperação e desempenho, recomenda-se que esses locais estejam em dispositivos de E/S diferentes.

- Arquivos de dados
- Arquivos de índice
- Arquivos de dados de resumo
- Arquivos de índice de resumo
- Arquivos de registro

Digite o local de armazenamento dos arquivos de banco de dados a seguir.

Diretório de Dados:	C:\Programas\esecdata
Diretório de Índices:	C:\Programas\esecdata
Diretório dos Dados de Resumo:	C:\Programas\esecdata
Diretório de Índice de Resumo:	C:\Programas\esecdata
Diretório de Registro:	C:\Programas\esecdata

15. Digite o tamanho do banco de dados:
    - Padrão (20.000 MB) – capacidade para 30 dias com 500.000 eventos por dia
    - Grande (400.000 MB) – capacidade para 30 dias com 10.000.000 eventos por dia
    - Personalizado (especifique manualmente o tamanho). Se escolher essa opção, você será solicitado a fornecer:
      (1) o tamanho do banco de dados em MB (de 10.000 a 2.000.000)
      (2) o tamanho de cada arquivo de registro em MB (de 100 a 100.000)
      (3) o tamanho máximo de cada arquivo de banco de dados em MB
      (de 2.000 a 100.000)

16. Para o administrador do banco de dados do Sentinel, selecione:
    - Autenticação do Servidor SQL (esecdba), a senha e a confirmação da senha, ou
    - Autenticação do Windows e digite <nome_do_domínio>\<nome_do_usuário>

    NOTA: Se você selecionar *Autenticação do Servidor SQL*, não poderá modificar o nome de login padrão.

    Digite as informações de autenticação do usuário do Administrador do Banco de Dados do Sentinel (DBA).

    Autenticação do Windows

    Autenticação do Servidor SQL

    Login:

    Autenticação do Windows

    Digite as informações de autenticação do usuário do Administrador do Banco de Dados do Sentinel (DBA).

    Autenticação do Windows

    Autenticação do Servidor SQL

    Login: esecdba

    Palavra-passe:

    Confirmar Senha:

    Autenticação do SQL Server

    NOTA: No caso de autenticação do SQL, o instalador não continuará a menos que a senha esecdba corresponda à senha esecdba da v4.2.

    ---

17. Para o usuário do banco de dados do aplicativo Sentinel. Selecione uma destas opções:
    - *Autenticação do Servidor SQL* (esecapp), digite a senha e a confirmação da senha
    - *Autenticação do Windows*, digite <nome_do_domínio>\<nome_do_usuário>, a senha e a confirmação da senha

    ---
    NOTA: Se você selecionar *Autenticação do Servidor SQL*, não poderá modificar o nome de login padrão.

Digite as informações de autenticação do usuário do Banco de Dados de Aplicativo do Sentinel.

Autenticação do Windows

Autenticação do Servidor SQL

Login:

Palavra-passe:

Confirmar Senha:

Autenticação do Windows

Digite as informações de autenticação do usuário do Banco de Dados de Aplicativo do Sentinel.

Autenticação do Windows

Autenticação do Servidor SQL

Login: esecapp

Palavra-passe:

Confirmar Senha:

Autenticação do SQL Server

18. Para o usuário Administrador do Sentinel. Selecione uma destas opções:
    - *Autenticação SQL*, digite o nome de usuário do Administrador do Sentinel (padrão: esecadm), a senha e a confirmação da senha
    - *Autenticação do Windows* e digite <nome_do_domínio>\<nome_do_usuário>

NOTA: Se você selecionar *Autenticação do Servidor SQL*, não poderá modificar o nome de login padrão.

Digite as informações de autenticação do usuário do Administrador do Sentinel.

Autenticação do Windows

Autenticação do Servidor SQL

Login:

Autenticação do Windows

Digite as informações de autenticação do usuário do Administrador do Sentinel.

Autenticação do Windows

Autenticação do Servidor SQL

Login: esecadm

Palavra-passe:

Confirmar Senha:

Autenticação do SQL Server

19. Para o usuário do Gerador de Relatórios do Sentinel. Selecione uma destas opções:

NOTA: Para o Gerador de Relatórios do Sentinel, a Autenticação do Windows exige que você esteja executando o Crystal Enterprise Professional. O Professional permite criar contas e mapas diferentes, de acordo com a necessidade. Se você estiver usando a versão Standard, selecione *Autenticação SQL*.

- *Autenticação SQL* (esecrpt), digite a senha e a confirmação da senha
- *Autenticação do Windows* e digite <nome_do_domínio>\<nome_do_usuário>

NOTA: Se você selecionar *Autenticação do Servidor SQL*, não poderá modificar o nome de login padrão.

Digite as informações de autenticação do usuário do Sentinel Report.

Autenticação do Windows

Autenticação do Servidor SQL

Login:

Autenticação do Windows

Digite as informações de autenticação do usuário do Sentinel Report.

Autenticação do Windows

Autenticação do Servidor SQL

Login: esecrpt

Palavra-passe:

Confirmar Senha:

Autenticação do SQL Server

20. Clique em *Avançar* na janela de resumo da instalação do banco de dados.
21. Depois de concluída a instalação, será necessário reinicializar. Clique em *Concluir* para reinicializar o sistema.

Migração

O utilitário de migração de dados migra apenas os seguintes itens:

- Usuários e permissões designadas
- Filtros
- Opções de configuração do menu popup.
- Tags CV renomeadas
- Configurações de arquivo e partição
- Os casos da v4.2 são copiados na v5 como incidentes
- Incidentes e eventos relacionados a incidentes

NOTA: O utilitário de migração de dados NÃO migrará dados de eventos, exceto quando os dados do evento estiverem associados a incidentes. Só será feita a migração dos dados de evento associados a incidentes.

NOTA: Os dados de evento de incidente não podem ser vistos no Sentinel Control Center. Esses dados podem ser exibidos usando o Crystal Reporting ou consultas ao SQL.

Migração de dados para bancos de dados do Sentinel 5 quando o Administrador do Banco de Dados do Sentinel é um usuário da Autenticação do Windows.

NOTA: Este procedimento se aplica a instalações de banco de dados do Sentinel 5 em que o Administrador do Banco de Dados do Sentinel (equivalente a esecdba) é um usuário da Autenticação do Windows. Este procedimento adiciona um usuário esecdba da Autenticação SQL ao banco de dados do Sentinel 5 para que os dados da v4.2 possam ser migrados para a v5.

1. Efetue login como um usuário com direitos administrativos.
2. Inicie o MS SQL Server Query Analyzer. Efetue login como o usuário sa ou o usuário equivalente da Autenticação do Windows.
3. Clique em *File* (Arquivo) > *Open* (Abrir). Navegue até:

```
%ESEC_HOME%\utilities\db\scripts\ddl\mssql\Migration
```

4. Selecione import_add_esecdba.sql.
5. Clique em *Abrir*.
6. Clique em *Query* (Consulta) > *Execute* (Executar).
7. Depois de concluído o script, saia do Query Analyzer.

NOTA: Depois de executar a migração dos dados, você pode usar o MS SQL Server Enterprise Manager para excluir esse usuário esecdba da Autenticação SQL do banco de dados do Sentinel 5.

Migração de dados

1. Efetue login como um usuário com direitos administrativos.
2. Verifique as variáveis de ambiente para garantir que o java (versão 1.4.2) está na variável PATH. Para realizar essa verificação, execute este comando na linha de comando:

   ```
   java -version
   ```

   Se esse comando não tiver êxito, localize onde o java foi instalado no sistema ou faça o download e instale o java. Em seguida, atualize a variável de ambiente PATH para incluir o executável do java. Por exemplo, se o java estiver instalado no diretório:

   ```
   C:\Arquivos de Programas\sentinel5.1.3.0\Sun-1.4.2
   ```

   Adicione o seguinte no início da variável de ambiente PATH:

   ```
   C:\Arquivos de Programas\sentinel5.1.3.0\Sun-1.4.2\bin;
   ```

3. No prompt de comando, use o comando cd para mudar para o diretório a seguir no CD de instalação do software Sentinel 5:

   ```
   sentinel\dbsetup\bin
   ```

4. Execute o comando:

   ```
   .\MigrateDb.bat
   ```

5. Você será solicitado a fornecer o seguinte:
   - O nome do host do banco de dados (no qual os bancos de dados do Sentinel 4.2 e do Sentinel 5 estão sendo executados)
   - O nome do banco de dados de destino (do banco de dados do Sentinel 5 para o qual está migrando)
   - A senha do esecdba (que deve ser idêntica à do usuário esecdba nos bancos de dados do Sentinel v4.2 e v5)
   - O nome do banco de dados de origem (nome do banco de dados v4.2)
   - O diretório de registro (no qual os arquivos de registro da migração de dados serão colocados)
   - A opção de migração:
     - (1) Configurações do sistema
     - (2) Incidentes/casos
     - (3) Ambos
     - (4) Nenhum

NOTA: A migração das configurações do sistema deve ser executada com êxito para poder migrar incidentes e casos.

NOTA: Se houver falha na migração das configurações do sistema, desinstale o banco de dados do Sentinel 5 selecionando a opção *Apagar apenas os objetos de banco de dados*. Em seguida, reinstale o banco de dados do Sentinel 5 com a opção *Adicionar objetos de banco de dados a um banco de dados vazio existente*. Por último, repita as instruções da migração de dados.

NOTA: Se houver falha da migração de incidentes, execute-a novamente. O utilitário de migração será reiniciado no ponto da falha. Não será necessário executar tarefas adicionais de limpeza.

NOTA: Depois de executar a migração dos dados, você poderá usar o MS SQL Server Enterprise Manager para excluir o usuário esecdba da Autenticação SQL do banco de dados do Sentinel 5, caso tenha sido necessário adicioná-lo para o Utilitário de Migração de Dados.

Pós-migração - Instalando o Sentinel 5

No Sentinel 5, os seguintes recursos são novos, diferentes ou foram removidos.

- iTRAC – esta é uma funcionalidade nova. As permissões de usuário associadas são:

- Incidentes – foi adicionada a Administração de Incidentes. Todas as funcionalidades relacionadas a casos foram removidas. As permissões de usuário associadas são:

Incidentes do Sentinel v4.2

Incidents
View Incidents Tab
Incident Administration
View Incident(s)
Create Incident(s)
Modify Incident(s)
Delete Incident(s)
Assign Incident(s)
Email Incidents
Incident Actions

Incidentes do Sentinel v5

- Gerenciamento de Coletor – na v4.2 chamava-se Monitoramento de Assistente. Guia *Exibir Assistentes* mudou para *Exibir Coletores*. *Controlar Assistentes e Coletor* mudou para *Controlar Coletores* e *Administração do Coletor*. As permissões de usuário associadas são:

Wizard Monitoring
View Wizards Tab
Control Wizards and Agents

Monitoramento de Assistente do Sentinel v4.2

Collector Management
View Collectors
Control Collectors
Collector Administration

Gerenciamento de Coletor do Sentinel v5

- Administração – adição de Estatísticas do DAS, Gerenciamento de Sessão de Usuário e Gerenciamento de Função do iTRAC. *Regras de Correlação* foi renomeado para *Correlação*. O recurso Configuração de Evento foi movido para o Gerenciador de Dados do Sentinel. *Configuração do Usuário* foi renomeado como *Gerenciamento do Usuário*. As permissões de usuário associadas são:

Administração do Sentinel v4.2 | **Administração do Sentinel v5**

- ActiveViews™ - na v4.2, chamava-se Tempo Real. *Exibições de Resumo* foi renomeado como *Active Views*. As permissões de usuário associadas são:

Tempo Real do Sentinel v4.2 | **Active Views™ do Sentinel v5**

- A funcionalidade Visão Geral do Sistema não está disponível no Sentinel 5.

Instalando o Sentinel 5

1. Instale o Sentinel 5, consulte o capítulo sobre instalação *Instalando o Sentinel para Windows*.
2. Instale o Service Pack mais recente do Sentinel.
3. Execute as etapas a seguir se quiser adicionar novas funcionalidades para os usuários existentes da v4.2:
   a. Verifique se o *Sentinel Server* está em execução.
   b. Faça login no Sentinel Control Center como usuário com permissão de Administração/Gerenciamento de Usuário (por exemplo, esecadm).
   c. No Sentinel Control Center, clique na guia Admin. Expanda Configuração do Usuário no painel Navegação ou, na barra de navegação, clique em *Admin > Configuração do Usuário*.
   d. Clique o botão direito do mouse no usuário ao qual deseja adicionar a funcionalidade (por exemplo, esecadm) e selecione *Detalhes do Usuário*. Clique na guia *Permissões*.
   e. Expanda iTRAC e atribua as permissões de acordo com a necessidade.
   f. Expanda Incidentes e atribua *Administração de Incidentes* de acordo com a necessidade.

g. Expanda Gerenciamento de Coletor e atribua *Administração do Coletor* conforme o necessário.
h. Expanda Administração e atribua *Estatísticas do DAS*, *Gerenciamento de Sessão de Usuário* ou *Gerenciamento de Função do iTRAC* conforme o necessário.
i. Clique na guia *Funções* e atribua a *Função de Workflow Admin* ou *Analista*, conforme o necessário.
j. Clique em *OK*.

4. Se aplicável, importe as regras de correlação. Os conjuntos de regras exportados do Sentinel 4.2 aparecerão como pastas de regras quando importados para o Sentinel 5.
5. Copie do backup os scripts de Coletor e configurações de porta seguindo as instruções na seção Pós-migração – Reconfigurando scripts de coletor e configurações de porta

Pós-migração – reconfigurando scripts de coletor e configurações de porta

Em cada máquina na qual o Sentinel 5 Collector Service (Gerenciador de Coletor) estiver instalado, execute as etapas a seguir para restabelecer os scripts de coletor e as configurações de porta que foram usados na instalação do Sentinel v4.2.

Para restabelecer os scripts de coletor e as configurações de porta

1. Pare o serviço Gerenciador de Coletor Windows.
2. No local em que você colocou um backup do diretório %WORKBENCH_HOME%\Agents da instalação do Sentinel v4.2, copie os seguintes arquivos para o diretório %WORKBENCH_HOME%\Agents da instalação atual do Sentinel 5 (sobregrave os arquivos, se necessário):
   - localhost_portcfg.dat
   - localhost_snmpcfg.dat
3. Leia o arquivo de texto criado durante a Pré-migração que lista todos os coletores usados pela instalação do Gerenciador de Coletor do Sentinel v4.2 nesta máquina. Você precisará saber os nomes de coletor para executar a próxima etapa.
4. No local em que você colocou um backup do diretório %WORKBENCH_HOME%\Elements da instalação do Sentinel v4.2, copie os diretórios cujos nomes correspondem aos nomes do coletor no arquivo de texto no diretório %WORKBENCH_HOME%\Elements da instalação atual do Sentinel 5 (sobregrave os arquivos e diretórios, se necessário).
5. Obtenha o utilitário UpgradePortCfgFile no site de Suporte Técnico do Sentinel (faça o download aqui).
6. Extraia o arquivo ZIP UpgradePortCfgFile.
7. Abra um prompt de comando e mude os diretórios no diretório do utilitário UpgradePortCfgFile extraído. Nesse diretório, execute o comando:

```
.\UpgradePortCfgFile.bat
```

8. Inicie o serviço Gerenciador de Coletor.

Pós-migração – Configurando o Sentinel 5 para o Crystal Reporting

Se você estiver executando Crystal Reports para Sentinel 4.2 e quiser executar Crystal Reports com o Sentinel 5, será preciso:

- Modificar as configurações ODBC relacionadas ao Crystal Reports para que apontem para o banco de dados do Sentinel 5.
- Importar os gabaritos do Crystal Report (incluindo os gabaritos de migração de dados) do Service Pack mais recente.

Consulte o capítulo sobre instalação *Crystal Reports* para obter mais informações.

Patch da v5.x.x até a v5.1.3

Execute este procedimento em qualquer máquina que tenha componentes do Sentinel instalados.

Patch do Sentinel v5.x.x para v5.1.3 quando o administrador do banco de dados do Sentinel (esecdba) é um login de Autenticação do SQL Server

Fazendo upgrade da v5.x.x para a v5.1.3 no caso de Autenticação do SQL Server

NOTA: Se você estiver executando a v5.1.1sp1 ou superior e fez alterações no arquivo syslog.conf, será necessário fazer uma cópia do arquivo syslog.conf. O instalador de patch sobregravará o arquivo syslog.conf. Após aplicar o patch, modifique ou sobregrave o novo arquivo syslog.conf para corresponder ao arquivo syslog.conf. original.

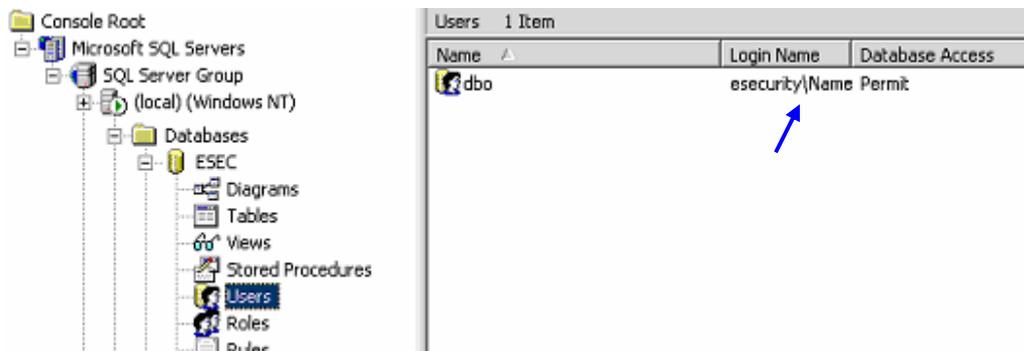
1. Feche todos os Sentinel Control Centers, Gerenciadores de Dados do Sentinel e Construtores de Coletor que estiverem abertos.
2. Insira o CD de instalação de patch do Sentinel na unidade de CD-ROM.
3. Procure o diretório de patch apropriado.
4. No diretório de patch, clique duas vezes em *setup.bat*.

NOTA: No momento, não há suporte no Windows para a instalação no modo de console.

5. Na tela de boas-vindas, clique em *Avançar*.
6. Aceite o Contrato de Licença de Usuário Final e clique em *Avançar*.
7. Clique em *Avançar* até chegar à janela de informações do banco de dados.
8. Verifique se o tipo do banco de dados está correto. Selecione o local do diretório do registro de instalação do banco de dados. Clique em *Avançar*.
9. Verifique se as informações do MS SQL Server estão corretas. Selecione *Autenticação do Servidor SQL*. Digite o nome do usuário esecdba e a senha. Clique em *Avançar*.
10. Clique em *Instalar*. Talvez você seja solicitado a reinicializar a máquina. Caso contrário, reinicia os Serviços do Sentinel (*Gerenciador de Coletor, Sentinel e Comunicações do Sentinel*).

Patch do Sentinel v5.x.x para v5.1.3 quando o administrador do banco de dados do Sentinel é a Autenticação do Windows

No caso da Autenticação do Windows, o InstallShield do patch não aplicará o patch do banco de dados. O instalador do patch do banco de dados deve ser executado como o usuário esecdba do domínio Windows para o banco de dados do Sentinel.

Ao executar o instalador do patch na máquina em que você instalou originalmente o componente Banco de Dados, será preciso saber o nome do usuário e a senha do usuário administrador do banco de dados do Sentinel (esecdba). Para determinar o usuário esecdba, localize o Nome de Login do usuário dbo do banco de dados do Sentinel usando o SQL Server Enterprise Manager, como mostrado a seguir.

Durante o processo do patch, você receberá uma mensagem popup informando que o patch do banco de dados deve ser executado via linha de comando, como explicado a seguir.

Patch da v5.x.x para v5.1.3 no caso de Autenticação do Windows

NOTA: Se você estiver executando a v5.1.1sp1 ou superior e fez alterações no arquivo syslog.conf, será necessário fazer uma cópia do arquivo syslog.conf. O instalador de patch sobregravará o arquivo syslog.conf. Após aplicar o patch, modifique ou sobregrave o novo arquivo syslog.conf para corresponder ao arquivo syslog.conf. original.

1. Feche todos os Sentinel Control Centers, Gerenciadores de Dados do Sentinel e Construtores de Coletor que estiverem abertos.
2. Insira o CD de instalação de patch do Sentinel na unidade de CD-ROM.
3. Procure o diretório de patch apropriado.
4. No diretório de patch, clique duas vezes em *setup.bat*.

NOTA: No momento, não há suporte no Windows para a instalação no modo de console.

5. Na tela de boas-vindas, clique em *Avançar*.
6. Aceite o Contrato de Licença de Usuário Final e clique em *Avançar*.
7. Clique em *Avançar* até chegar à janela de informações do banco de dados.
8. Verifique se o tipo e o nome do banco de dados estão corretos. Selecione o local do diretório do registro de instalação do banco de dados. Clique em *Avançar*.

A seguinte mensagem popup será exibida. Leia a mensagem e clique em *OK* para continuar.

9. Verifique se as informações do MS SQL Server estão corretas. Selecione *Autenticação do Windows*. Digite seu nome de usuário e sua senha para o usuário do Aplicativo do Sentinel. Clique em *Avançar*.

CUIDADO: A máquina do banco de dados NÃO DEVE SER REINICIALIZADA NO FINAL DA INSTALAÇÃO.

10. Na janela de resumo, clique em *Instalar*.
11. Na máquina do banco de dados, saia do InstallShield sem reinicializá-la.
12. Se ainda não tiver feito isto, na máquina do banco de dados, efetue login como o usuário esecdba do Domínio Windows.
13. Abra um prompt de comando.
14. Verifique as variáveis de ambiente para garantir que o java (versão 1.4.2) está na variável PATH. Para realizar essa verificação, execute este comando na linha de comando:

```
java -version
```

Se esse comando não tiver êxito, localize onde o java foi instalado no sistema ou faça o download e instale o java. Em seguida, atualize a variável de ambiente PATH para incluir o executável do java. Por exemplo, se o java estiver instalado no diretório:

```
C:\Arquivos de Programas\sentinel5.1.3.0\Sun-1.4.2
```

Adicione o seguinte no início da variável de ambiente PATH:

```
C:\Arquivos de Programas\sentinel5.1.3.0\Sun-1.4.2\bin;
```

15. No prompt de comando, mude para o seguinte diretório no CD de instalação do Sentinel:

```
<Diretório de patch>\sentinel\dbsetup\bin
```

16. Digite o comando:

```
.\PatchDb.bat
```

17. No prompt, digite o nome do host ou o endereço IP estático do SQL Server do banco de dados do Sentinel ao qual deseja aplicar o patch.

18. No prompt, digite o nome do banco de dados do Sentinel do SQL Server ao qual deseja aplicar o patch.
19. No prompt, digite a opção 1 para Autenticação do Windows. O script verificará as informações digitadas e iniciará o patch do banco de dados.
20. Depois que o script concluir a aplicação do patch, reinicialize os serviços.

Atualizando o conector syslog

Se estiver usando os scripts do conector syslog de uma versão anterior do Sentinel para 5.1.1.1 (ou seja - 5.0, 5.0.1.0, 5.1.0.0, ou 5.1.1.0) você deve iniciar usando os scripts do conector de syslog que está incluído no patch. Para alternar o uso do script do conector syslog antigo para os scripts do conector syslog novo, remova o script antigo e instale o novo script.

O conector syslog é instalado com scripts que são executados no Windows e UNIX com arquivos de configuração aprimorados. Além disso, a instalação do servidor proxy syslog como um serviço foi simplificada.

Para remover o conector syslog

1. Efetue login como Administrador.
2. cd d/ %ESEC_HOME%\wizard\/syslog
3. Digite:

```
.\syslog-server.bat remove
```

Para instalar o conector syslog

1. Efetue login como Administrador.
2. cd d/ %ESEC_HOME\wizard\syslog
3. .\syslog-server.bat install
4. Se você fez alterações no arquivo syslog.conf da instalação original, será necessário modificar ou sobregravar o novo arquivo syslog.conf para refletir o arquivo syslog.conf original. Ele está localizado em:

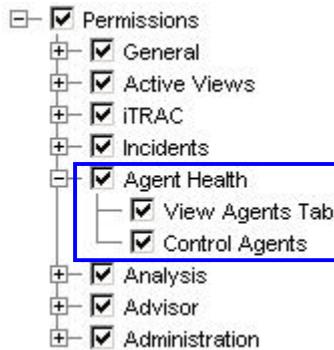
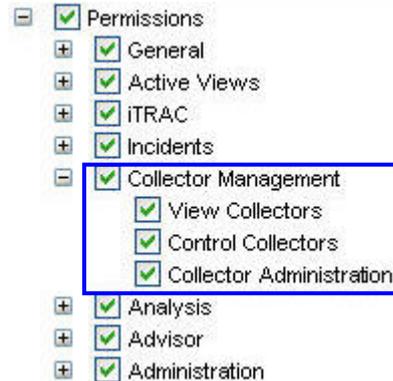
```
%ESEC_HOME%\wizard\syslog\config
```

Atualizando as Permissões do Usuário para a v5.0.x até a v5.1.3

Durante o upgrade da v5 ou v5.0.1 para a v5.1.3, a Saúde do Coletor foi mudada para Gerenciamento de Coletor com a inclusão de uma funcionalidade adicional de Administração de Coletor. Além disso, a funcionalidade Telas de Servidor foi adicionada. Opcionalmente, você pode conceder essa permissão.

Atualizando as permissões de Gerenciamento do Usuário

1. Faça login no Sentinel Control Center como usuário com permissão de Administração/Gerenciamento de Usuário.

Na v5.1, a Saúde do Coletor em Permissões foi mudada de *Saúde do Coletor* para *Gerenciamento de Coletor* com a inclusão de uma permissão adicional.

Permissão de usuário do Sentinel v5.0

Permissão de usuário do Sentinel v5.1

2. No Sentinel Control Center, clique na guia *Admin*. Expanda Configuração do Usuário no painel Navegação ou, na barra de navegação, clique em *Admin* > *Configuração do Usuário*.
3. Clique o botão direito do mouse em um usuário Admin (ou seja, esecadm ou outro usuário admin) > *Detalhes do Usuário*. Clique na guia *Permissões*.
4. Expanda Gerenciamento de Coletor e atribua *Administração do Coletor*. Clique em *OK*.

Atualizando as permissões de Tela de Servidor

Para usar a tela de servidor após a instalação do patch, é necessário conceder a permissão *Telas de Servidor* ao usuário do Sentinel que esteja usando o Gerenciador do Usuário. O Gerenciador do Usuário fica localizado sob a guia Admin do Sentinel Control Center.

Crystal Reporting Server

Depois de fazer o upgrade para o Sentinel v5.1.3, incluindo a aplicação do Service Pack mais recente, você deverá importar os relatórios do Service Pack mais atual. Consulte o capítulo 'Crystal Reports' no Guia de Instalação para obter mais informações.

Atualizando o e-mail do Sentinel para autenticação SMTP

Se o sistema exigir autenticação SMTP, você precisará atualizar o arquivo execution.properties. Esse arquivo está na máquina em que o DAS foi instalado. Ele está localizado em %ESEC_HOME%\sentinel\config. Para configurar esse arquivo, execute mailconfig.bat para mudar o arquivo e mailconfigtest.bat para testar as mudanças.

Para configurar o arquivo execution.properties

5. Na máquina em que o DAS foi instalado, faça login como esecadm e mude para o diretório:

```
%ESEC_HOME%\sentinel\config
```

6. Execute mailconfig desta maneira:

```
mailconfig.bat -host <servidor SMTP> -from <endereço de
   e-mail de origem> -user <usuário de autenticação de
   e-mail> –password
```

Exemplo:

```
mailconfig.bat -host 10.0.1.14 -from meu_nome@domínio.com
   -user meu_nome_de_usuário –password
```

Depois de digitar esse comando, você será solicitado a fornecer uma nova senha.

```
Digite a senha:*********
```

```
Confirme a senha:*********
```

NOTA: Ao usar a opção password, ela deve ser o último argumento.

Para testar a configuração de execution.properties

7. Na máquina em que o DAS foi instalado, mude para o diretório:

```
%ESEC_HOME%\sentinel\config
```

8. Execute mailconfigtest desta maneira:

```
mailconfigtest.bat -to <endereço de e-mail de destino>
```

Se o e-mail for enviado com êxito, será exibida a seguinte mensagem na tela e o e-mail será recebido no endereço de destino.

```
O e-mail foi enviado com êxito!
```

Verifique a caixa de correio do e-mail de destino para confirmar o recebimento da mensagem. A linha de assunto e o conteúdo devem ser:

```
Assunto: Testando a propriedade de e-mail do Sentinel
```

```
Este é um teste da configuração da propriedade de e-mail
   do Sentinel. Se você vir esta mensagem, a propriedade
   de e-mail do Sentinel foi configurada corretamente
   para enviar e-mail
```

8 Patch para Oracle no Linux

NOTA: O termo Agente é sinônimo de Coletor. De agora em diante, Agentes serão referidos como Coletores.

Este capítulo discute os patches v5.1.1.1 a v5.1.3.

Patch da v5.1.1.1 para a v5.1.3

Execute este procedimento em qualquer máquina que tenha componentes do Sentinel instalados.

Se estiver executando o instalador de patches na máquina em que o componente Banco de Dados foi instalado originalmente, você precisará saber a senha do usuário administrador do banco de dados do Sentinel (esecdba).

Fazendo upgrade da v5.1.1.1 para v5.1.3 para o Linux

1. Faça login como usuário Root.

   NOTA: Se você fez alterações no arquivo syslog.conf na instalação de v5.1.1.1, será necessário fazer uma cópia desse arquivo. O instalador de patch sobregravará o arquivo syslog.conf. Após aplicar o patch, modifique ou sobregrave o novo arquivo syslog.conf para corresponder ao arquivo syslog.conf. original.

2. Insira e monte o CD de patch do Sentinel.
3. Para iniciar o programa de instalação, vá para o diretório de patch apropriado no CD-ROM e execute o comando:

   Para o modo de interface gráfica:

   ```
   ./setup.sh
   ```

   ou

   Para modo textual:

   ```
   ./setup.sh –console
   ```

4. Na tela de boas-vindas, clique em *Avançar*.
5. Aceite o Contrato de Licença de Usuário Final e clique em *Avançar*.
6. Clique em *Avançar* até chegar à janela de informações do banco de dados.
7. Verifique se o tipo do banco de dados está correto. Selecione o local do diretório do registro de instalação do banco de dados. Clique em *Avançar*.
8. Verifique se as informações do servidor Oracle estão corretas. Digite a senha do esecdba. Siga os outros prompts do instalador.

Atualizando o conector syslog

Se estiver usando os scripts do conector syslog de uma versão anterior do Sentinel para 5.1.1.1 (ou seja - 5.0, 5.0.1.0, 5.1.0.0, ou 5.1.1.0) você deve iniciar usando os scripts do conector de syslog que está incluído no patch. Para alternar o uso do script do conector syslog antigo para os scripts do conector syslog novo, remova o script antigo e instale o novo script.

O conector syslog é instalado com scripts que são executados no Windows e UNIX com arquivos de configuração aprimorados. Além disso, a instalação do servidor proxy syslog como um serviço foi simplificada.

Para remover o conector syslog

1. Efetue login como Usuário Root.
2. cd $ESEC_HOME/wizard/syslog
3. ./syslog-server.sh remove

Para instalar o conector syslog

1. Efetue login como Usuário Root.
2. cd $ESEC_HOME/wizard/syslog
3. ./syslog-server.sh install
4. Se você fez alterações no arquivo syslog.conf da instalação original, será necessário modificar ou sobregravar o novo arquivo syslog.conf para refletir o arquivo syslog.conf original. Ele está localizado em:

```
$ESEC_HOME/wizard/syslog/config
```

Crystal Reporting Server

Depois de fazer a atualização para o Sentinel 5.1.3, incluindo a aplicação do Service Pack mais recente (se houver), você deve importar os relatórios do Service Pack mais atual. Para obter mais informações, consulte o capítulo sobre o Crystal Reports, no Guia de Instalação.

Atualizando o e-mail do Sentinel para autenticação SMTP

Se o sistema exigir autenticação SMTP, você precisará atualizar o arquivo execution.properties. Esse arquivo está na máquina em que o DAS foi instalado. Ele está localizado em $ESEC_HOME/sentinel/config. Para configurar esse arquivo, execute mailconfig.sh para mudar o arquivo e mailconfigtest.sh para testar as mudanças.

Para configurar o arquivo execution.properties

1. Na máquina em que o DAS foi instalado, faça login como esecadm e mude para o diretório:

```
$ESEC_HOME/sentinel/config
```

2. Execute mailconfig desta maneira:

```
./mailconfig.sh -host <servidor SMTP> -from <endereço
  de e-mail de origem> -user <usuário de autenticação
  de e-mail> –password
```

Exemplo:

```
./mailconfig.sh -host 192.0.2.14 -from
   meu_nome@domínio.com -user meu_nome_de_usuário –
   password
```

Depois de digitar esse comando, você será solicitado a fornecer uma nova senha.

```
Digite a senha:*********
```

```
Confirme a senha:*********
```

NOTA: Ao usar a opção password, ela deve ser o último argumento.

Para testar a configuração de execution.properties

1. Na máquina em que o DAS foi instalado, faça login como esecadm e mude para o diretório:

```
$ESEC_HOME/sentinel/config
```

2. Execute mailconfigtest desta maneira:

```
./mailconfigtest.sh -to <endereço de e-mail de destino>
```

Se o e-mail for enviado com êxito, será exibida a seguinte saída na tela e o e-mail será recebido no endereço de destino.

```
O e-mail foi enviado com êxito!
```

Verifique a caixa de correio do e-mail de destino para confirmar o recebimento da mensagem. A linha de assunto e o conteúdo devem ser:

```
Assunto: Testando a propriedade de e-mail do Sentinel
```

```
Este é um teste da configuração da propriedade de e-
   mail do Sentinel. Se você vir esta mensagem, a
   propriedade de e-mail do Sentinel foi configurada
   corretamente para enviar e-mail
```

9 Crystal Reports para Windows e Solaris

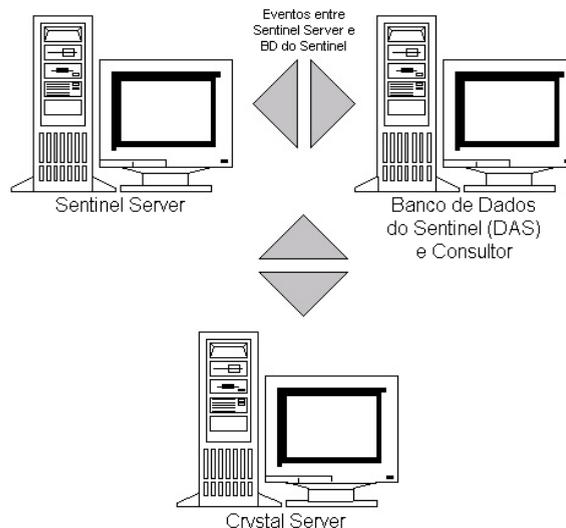
NOTA: O termo Agente é sinônimo de Coletor. De agora em diante, Agentes serão referidos como Coletores.

O Crystal BusinessObjects Enterprise™ 11 é uma ferramenta de geração de relatórios.

Este capítulo discute a configuração de instalação do Crystal Reports Server para Sentinel. A instalação deve ser feita na ordem apresentada.

- Instale o Microsoft IIS e o ASP.NET
- Instale o MS SQL (dependendo da configuração como autenticação do Windows ou autenticação do SQL Server)
- Instale o Crystal Server
  - Configurando o Open Database Connectivity (ODBC) para Autenticação SQL

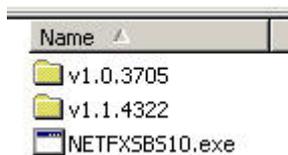
  ou

  - Instalando e configurando o software cliente do Oracle 9i
- Configure inetmgr
- Aplicação do patch do Crystal Reports;
- Publicação (importação) de Crystal Reports;
- Configurando uma conta 'Usuário Nomeado'
- Teste de conectividade com o servidor Web;
- Habilitando os relatórios dos Dez Melhores (opcional)
- Maximização de Relatórios de Eventos (recomendado);
- Configuração do Sentinel para o Crystal Enterprise Server.

Visão geral

O Crystal Reports Server requer um banco de dados para armazenar informações sobre o sistema e seus usuários. Esse banco de dados é conhecido como o banco de dados do Central Management Server (CMS). O CMS é um servidor que armazena informações sobre o sistema do Crystal Reports Server. Outros componentes do Crystal Reports Server podem acessar essas informações de acordo com a necessidade.

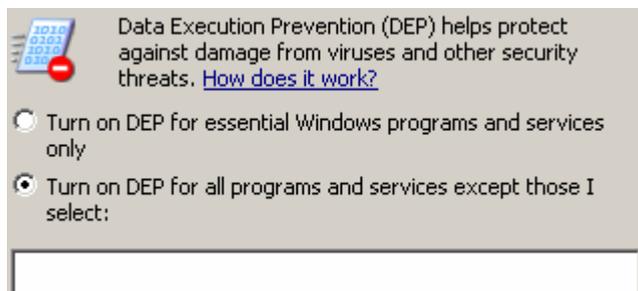
É preciso configurar um banco de dados CMS sobre um banco de dados MS SQL 2000 Server local. O instalador do Crystal Reports Server permite configurar o banco de dados CMS sobre o banco de dados MSDE se um MS SQL 2000 Server local não está instalado. O Sentinel 5 não tem suporte para uma configuração MSDE.

Requisitos do sistema

- Windows® 2003 Server com SP1 com uma partição formatada em NTFS com o IIS (Microsoft Internet Information Server) e o NET.ASP instalados. O Sentinel 5 não tem suporte para o Crystal XI no Windows® 2000 Server.
- .NET Framework 1.1 (instalado por padrão no Windows 2003. O BusinessObjects Enterprise™ 11 não tem suporte para o .NET Framework 2.0). Para determinar qual versão do .NET Framework está na máquina, vá para %SystemRoot%\Microsoft.NET\Framework. A pasta com o maior valor numérico não deve ser maior do que v.1.1.xxxx. Por exemplo:

Requisitos de configuração

1. Verifique se a conta usada para instalar o Crystal Reports Server tem direito de administrador local.
2. Defina a Prevenção de Execução de Dados (DEP) para ser executada em todos os programas e serviços selecionados. Isso é útil para evitar "Erro 1920. Serviço 'Crystal Report Cache Server' no Windows 2003".

   A DEP é acessada no *Painel de Controle* > *Sistema* > *guia Avançado* > *Configurações de Desempenho* > *Prevenção de Execução de Dados*.

   Selecione o botão '*Ativar a DEP para todos os programas e serviços, exceto os que eu selecionar:*'.

3. Se você planeja executar relatórios do Sentinel usando a autenticação do Windows NT, verifique se a conta do domínio Windows para o usuário do Sentinel Report já existe no banco de dados do Sentinel. Isso é feito durante a instalação do Sentinel, selecionando a *Autenticação do Windows* ao definir *Método de Autenticação para Usuário do Sentinel Report*, como mostra a ilustração a seguir.

Autenticação do Windows
Autenticação do Servidor SQL
Login:

4. Se você planeja executar relatórios do Sentinel usando a autenticação do SQL Server (também necessária para instalações do Sentinel Oracle), verifique se o login do SQL Server (esecrpt) já existe no banco de dados do Sentinel.
   - Para o banco de dados MS SQL do Sentinel - isso é feito durante a instalação do Sentinel para MS SQL, selecionando *Autenticação do Servidor SQL* ao definir *Método de Autenticação para Usuário do Sentinel Report*, como mostra a ilustração a seguir.

     Autenticação do Windows
     Autenticação do Servidor SQL
     Login: esecrpt
     Palavra-passe:
     Confirmar Senha:

   - Para o banco de dados Oracle do Sentinel – isso é feito durante a instalação do Sentinel para Oracle. O esecrpt recebe a mesma senha que esecadm.
5. Para Oracle - Oracle 9i Client Release 2 (9.2.0.1.0), instale isso antes de instalar o Crystal BusinessObjects Enterprise™ 11.
6. Para o MS SQL Server – instale o MS SQL 2000 sp3a antes de instalar o Crystal Reports Server 11.
7. Resolução de vídeo de 1024 x 768 ou superior
8. Instale o Microsoft Internet Information Server (IIS) e o NET.ASP

NOTA: O Sentinel 5 não tem suporte para o MSDE. Instale o MS SQL 2000 sp3a antes de instalar o Crystal Reports Server 11.

Instalando o Microsoft Internet Information Server (IIS) e o ASP.NET

Para adicionar esses componentes do Windows, talvez seja necessário usar o CD de instalação do Windows 2003 Server.

Instalando o IIS e o ASP.NET

1. No Windows, vá para *Painel de controle* > *Adicionar ou remover programas*.
2. No painel vertical esquerdo, clique em *Adicionar ou remover componentes do Windows*.
3. Selecione *Servidor de aplicativo*.

4. Clique em *Detalhes*.
5. Selecione *ASP.NET e Internet Information Services (IIS)*.

☑	ASP.NET	0.0 MB
☑	Enable network COM+ access	0.0 MB
☐	Enable network DTC access	0.0 MB
☑	Internet Information Services (IIS)	26.9 MB

6. Clique em *OK*.
7. Clique em *Avançar*. Você pode ser solicitado a usar o CD de instalação do Windows.
8. Clique em *Concluir*.

Problemas conhecidos

1. Instalando o Crystal Reports – você recebe duas chaves, uma para o Crystal Reports Server e outra para o Crystal Reports Developer. Use a chave do Crystal Reports Server ao instalar o Crystal Reports Server.
2. Desinstalando o Crystal Reports – caso seja necessário desinstalar o Crystal Reports Server, há um procedimento manual de desinstalação disponível que limpa as chaves do registro. Isso é útil quando a instalação é corrompida. Visite este site da BusinessObjects para obter os procedimentos para desinstalar manualmente o BusinessObjects Enterprise XI: http://support.businessobjects.com/library/kbase/articles/c2017905.asp.

   NOTA: Esse URL estava correto no momento da publicação deste documento.

3. Durante a configuração do .NET Administration Launchpad, ao mudar o nível de acesso de (*Inherited Rights*) (*Direitos Herdados*) para *View on Demand* (Ver por Demanda), o processo de atualização congela. Aguarde aproximadamente trinta segundos. O nível de acesso será atualizado.

Usando Crystal Reports

Para obter informações sobre como usar o Crystal Reports para geração de relatórios do Sentinel, consulte a *Documentação do Crystal Reports* e o *Guia do Usuário do Sentinel*.

Visão geral da instalação

Visão geral da instalação para MS SQL 2000 Server com Autenticação do Windows

Para instalar corretamente o Crystal Reports, execute os procedimentos a seguir na ordem apresentada.

1. Instale o Crystal Reports Server 11 – ao instalar o aplicativo Sentinel 5, se selecionar a *Autenticação do Windows* para o usuário do Relatório do Sentinel, siga o link Instalando o Crystal Server para MS SQL 2000 Server com Autenticação do Windows.
2. Configurar ODBC (Open Database Connectivity)
3. Mapeie o Crystal Reports para uso com o Sentinel
4. Aplique o patch do Crystal Reports
5. Publique relatórios
6. Defina o usuário como conta de usuário nomeado
7. Importe gabaritos do Crystal Reports
8. Crie uma página da Web Crystal (Configurando o .NET Administration Launchpad)
9. Configure o Sentinel para o Crystal Enterprise Server

Visão geral da instalação para MS SQL 2000 Server com Autenticação do Servidor SQL

Para instalar corretamente o Crystal Reports, execute os procedimentos a seguir na ordem apresentada.

1. Instale o Crystal Reports Server 11 – ao instalar o aplicativo Sentinel 5, se selecionar *Autenticação do Servidor SQL* para o usuário do Relatório do Sentinel, siga o link Instalando o Crystal Server para MS SQL 2000 Server com Autenticação do Servidor SQL ou para Oracle.
2. Configurar ODBC (Open Database Connectivity)
3. Mapeando o Crystal Reports para uso com o Sentinel
4. Importe gabaritos do Crystal Reports
5. Crie uma página da Web Crystal (Configurando o .NET Administration Launchpad)
6. Configure o Sentinel para o Crystal Enterprise Server

Visão geral da instalação para Oracle

Para instalar corretamente o Crystal Reports, execute os procedimentos a seguir na ordem apresentada.

1. Instale o cliente do Oracle 9i
2. Instale o Crystal Reports Server 11 – siga o link para instalar o Crystal Instalando o Crystal Server para MS SQL 2000 Server com Autenticação do Servidor SQL ou para Oracle.
3. Configurar driver nativo do Oracle
4. Mapeando o Crystal Reports para uso com o Sentinel

5. Importe gabaritos do Crystal Reports
6. Crie uma página da Web Crystal (Configurando o .NET Administration Launchpad)
7. Configure o Sentinel para o Crystal Enterprise Server

Instalação

Esta seção descreve como instalar o Crystal Server para:

- Banco de dados do MS SQL 2000 Server Sentinel com Autenticação do Windows
- Banco de dados do MS SQL 2000 Server Sentinel com Autenticação do Servidor SQL
- Banco de dados Oracle do Sentinel

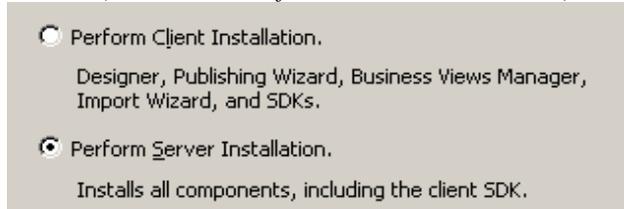
Instalando o Crystal Server para MS SQL 2000 Server com Autenticação do Windows

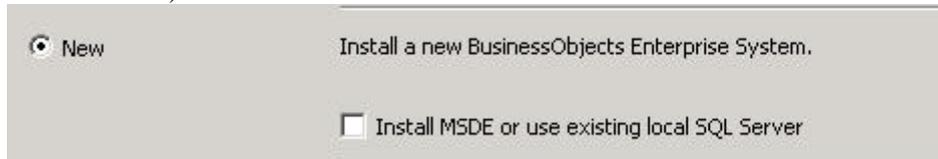
Instalação da Autenticação do Windows para o BOE XI Crystal Server

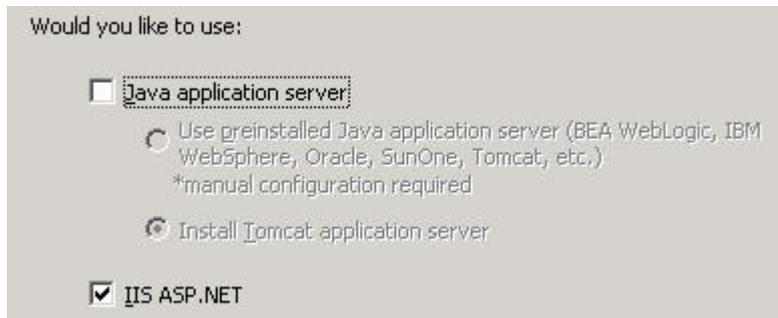
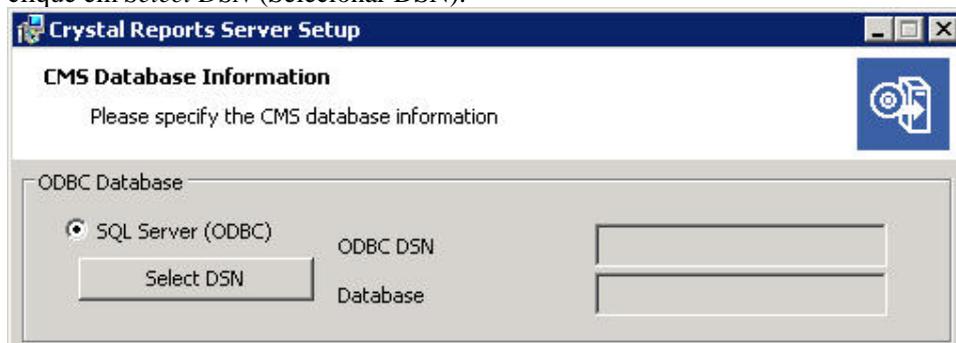
1. Instale o MS SQL 2000 sp3a em modo misto.
2. Inicie o MS SQL Enterprise Manager.
3. No painel de navegação, expanda (Windows NT) (local).
4. Realce e clique o botão direito em *Banco de Dados* e selecione *Novo Banco de Dados…*

5. Na guia Geral, no campo Nome, digite 'BOE11' e clique em *OK*.

6. Saia do MS SQL Enterprise Manager.
7. Insira o CD do BOE XI Crystal Server na unidade de CD-ROM.
8. Se a Reprodução Automática estiver desativada na máquina, execute *setup.exe*.

9. Na janela Select Client or Server Installation (Selecionar Instalação de Cliente ou Servidor), selecione *Perform Server Installation* (Executar Instalação de Servidor).

10. Como o tipo de instalação, selecione o botão *New* (Nova) e não marque '*Install MSDE or use existing local SQL Server*' (Instalar MSDE ou usar Servidor SQL local existente).

New
Install a new BusinessObjects Enterprise System.
Install MSDE or use existing local SQL Server

11. Na janela Web Component Adapter Type (Tipo de Adaptador de Componente Web), selecione *IIS ASP.NET*.

NOTA: Se você não tiver instalado o IIS e o ASP.NET usando o *Painel de Controle > Adicionar Remover Programas > Adicionar ou Remover Componentes do Windows*, o IIS ASP.NET ficará esmaecido.

12. Na janela 'CMS Database Information' (Informações do Banco de Dados CMS), clique em *Select DSN* (Selecionar DSN).

13. Clique na guia *Machine Data Source* (Fonte de Dados da Máquina).
14. Clique em *Novo*...

15. Selecione *System Data Source* (Fontes de Dados do Sistema).

   Select a type of data source:

   User Data Source (Applies to this machine only)

   System Data Source (Applies to this machine only)

   Clique em *Avançar*.

16. Role para baixo, selecione *Servidor SQL* e clique em *Avançar*.

   Select a driver for which you want to set up a data source.

Name	V
Microsoft FoxPro VFP Driver (*.dbf)	1
Microsoft ODBC for Oracle	2
Microsoft Paradox Driver (*.db)	4
Microsoft Paradox-Treiber (*.db)	4
Microsoft Text Driver (*.txt; *.csv)	4
Microsoft Text-Treiber (*.txt; *.csv)	4
Microsoft Visual FoxPro Driver	1
Microsoft Visual FoxPro-Treiber	1
SQL Server	2

17. Será exibida uma nova fonte. Clique em *Concluir*.

   System Data Source
   Driver: SQL Server

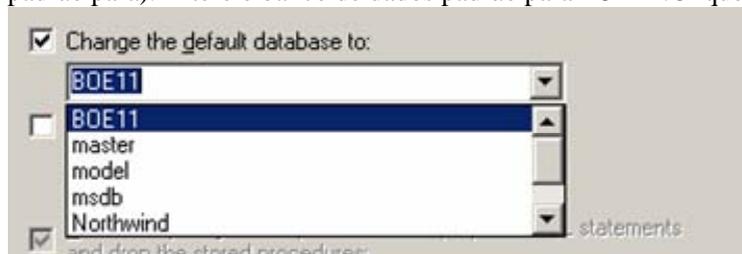
18. Na janela …*New Data Source to SQL Server* (Nova Fonte de Dados para Servidor SQL), digite:

   - Nome da fonte de dados (por exemplo, BOE_XI)
   - A descrição (opcional)
   - Para o servidor, clique na seta para baixo e selecione (*local*)

   Clique em *Avançar*.

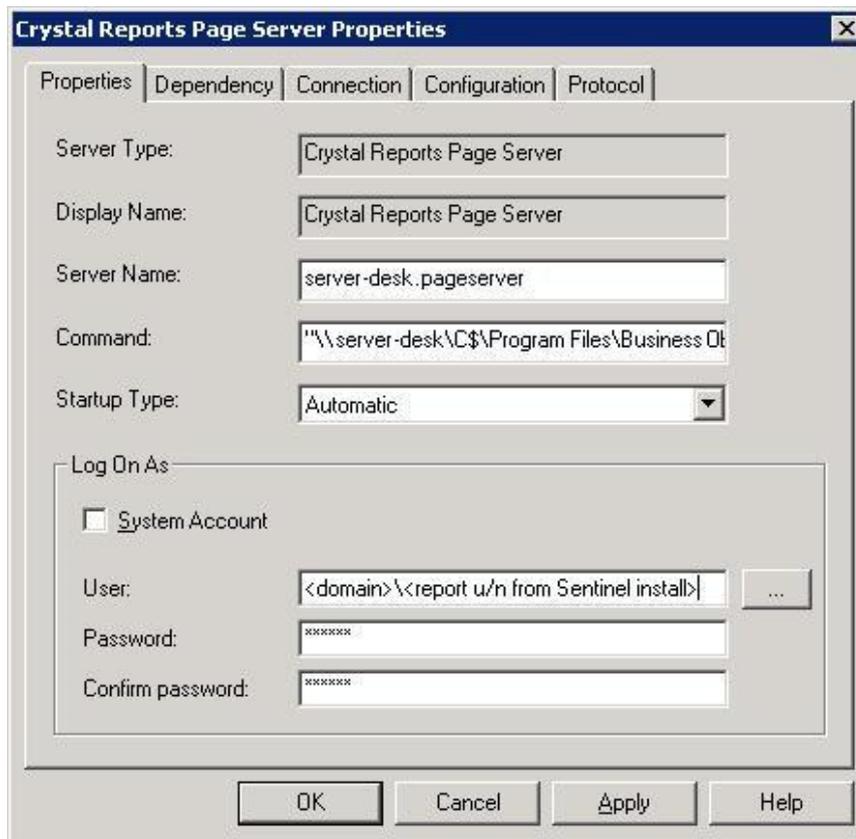
19. Se ainda não tiver feito isso, selecione *With Windows NT* … (com Windows NT). Clique em *Avançar*.

NOTA: A ID de login (esmaecida) é o seu nome de login no Windows.

20. Marque a caixa de seleção *Change the default database to*: (Mudar o banco de dados padrão para). Altere o banco de dados padrão para *BOE11*.Clique em *Avançar*.

21. Na janela 'Create a New Data Source to SQL Server' (Criar Nova Fonte de Dados para Servidor SQL), clique em *Concluir*.
22. Clique em *Testar Fonte de Dados*... Isso deve funcionar. Clique em *OK*.
23. Na janela Select Data Source (Selecionar Fonte de Dados), realce *BOE11* e continue a clicar em *OK* até exibir *SQL Server Login* (Login do Servidor SQL). Verifique se *Use Trusted Connection* (Usar Conexão Confiável) está selecionado. Clique em *OK*.

NOTA: A ID de login (esmaecida) é o seu nome de login no Windows.

24. Na janela de aviso, clique em *OK*.

25. Na janela 'CMS Database Information' (Informações do Banco de Dados CMS), clique em *Avançar*.
26. Clique em *Avançar* para continuar a instalação.
27. Após a instalação, será preciso mudar a conta de login para o Crystal Reports Page Server e o Crystal Reports Job Server para a conta de domínio do Usuário do Relatório do Sentinel.
    a. Clique em *Iniciar* > *Programas* > *BusinessObjects 11* > *Crystal Reports Server* > *Central Configuration Manager*.
    b. Clique o botão direito em *Crystal Reports Page Server* e selecione *Parar*.
    c. Clique novamente o botão direito em *Crystal Reports Page Server* e selecione *Propriedades*.
    d. Desmarque *Log On As System Account* (Fazer Logon como Conta do Sistema) e digite o nome de usuário e a senha do domínio do Usuário do Relatório do Sentinel usados durante a instalação do Sentinel 5. Clique em *OK*.

    e. Realce Crystal Reports Page Server, clique o botão direito do mouse para iniciar o Crystal Reports Page Server.

Configurando o Open Database Connectivity (ODBC) para Autenticação do Windows

Este procedimento configura uma fonte de dados ODBC entre o Crystal Reports no Windows e o Servidor SQL. Isso precisa ser realizado na máquina do Crystal Server.

Configurando uma fonte de dados ODBC para Autenticação do Windows

1. Vá para o *Painel de Controle do Windows > Ferramentas Administrativas > Fontes de Dados (ODBC)*.
2. Clique na guia *DSN de Sistema* e clique no botão *Adicionar*.
3. Selecione *Servidor SQL*. Clique em *Concluir*.
4. Será exibida uma tela solicitando as informações de configuração do driver:
   - Em Nome da Fonte de Dados, digite sentineldb
   - No campo Descrição (opcional), digite uma descrição
   - No campo Servidor, digite o nome do host ou o endereço IP do Sentinel Server

   Clique em *Avançar*.
5. Na tela seguinte, selecione *Autenticação do Windows*.

   NOTA: A ID de login (esmaecida) é o seu nome de login no Windows.
6. Na próxima tela, selecione:
   - Mude o banco de dados do Sentinel (o nome padrão é ESEC)
   - Deixe todas as configurações padrão

   Clique em *Avançar*.
7. Clique em *Concluir*.
8. Clique em *Test Data Source…* (Testar Fonte de Dados). Você deve conseguir estabelecer uma conexão. Clique em *OK* até sair.

Instalando o Crystal Server para MS SQL 2000 Server com Autenticação do Servidor SQL

Instale o Crystal Reports Server 11 com as seguintes opções selecionadas.

- Execute a instalação do servidor

- Instalar Novo BusinessObjects Enterprise System com 'Install MSDE or use existing local SQL Server' (Instalar MSDE ou usar Servidor SQL local existente).

NOTA: O Crystal Server e o MS SQL Server 2000 devem residir na mesma máquina.

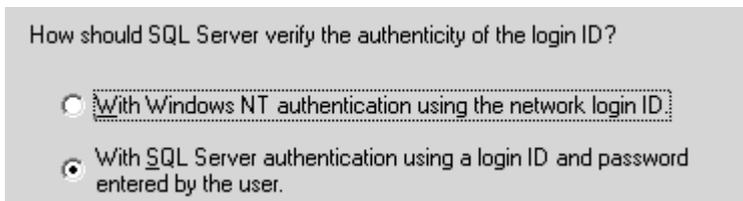
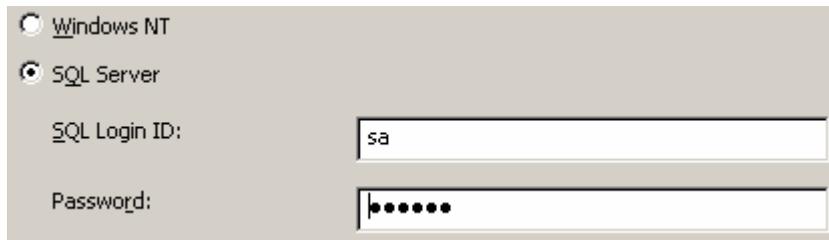
- IIS ASP.NET.

NOTA: Se você não tiver instalado o IIS e o ASP.NET usando o *Painel de Controle > Adicionar Remover Programas > Adicionar ou Remover Componentes do Windows*, o IIS ASP.NET ficará esmaecido.

- Você será solicitado a especificar o Modo de Autenticação. Selecione *Autenticação do Servidor SQL*.

How should SQL Server verify the authenticity of the login ID?

With Windows NT authentication using the network login ID.

With SQL Server authentication using a login ID and password entered by the user.

- Selecione *Autenticação do Servidor SQL*. Digite sa e a senha do sa.

Configurando o Open Database Connectivity (ODBC) para Autenticação SQL

Este procedimento configura uma fonte de dados ODBC entre o Crystal Reports no Windows e o Servidor SQL. Isso precisa ser realizado na máquina do Crystal Server.

Configurando uma fonte de dados ODBC para Windows

1. Vá para o *Painel de Controle do Windows* > *Ferramentas Administrativas* > *Fontes de Dados (ODBC)*.
2. Clique na guia *DSN de Sistema* e clique no botão *Adicionar*.
3. Selecione *Servidor SQL*. Clique em *Concluir*.
4. Será exibida uma tela solicitando as informações de configuração do driver:
   - Em Nome da Fonte de Dados, digite sentineldb
   - No campo Descrição (opcional), digite uma descrição
   - No campo Servidor, digite o nome do host ou o endereço IP do Sentinel Server

Clique em *Avançar*.

5. Na tela seguinte, selecione *Autenticação SQL*.
 Digite esecrpt como a ID de login e a senha. Clique em *Avançar*.

How should SQL Server verify the authenticity of the login ID?

With Windows NT authentication using the network login ID.

With SQL Server authentication using a login ID and password entered by the user.

To change the network library used to communicate with SQL Server, click Client Configuration.

Client Configuration...

Connect to SQL Server to obtain default settings for the additional configuration options.

Login ID: esecrpt

Password: ********

6. Na próxima tela, selecione:
   - Mude o banco de dados do Sentinel (o nome padrão é ESEC)
   - Deixe todas as configurações padrão

   Clique em *Avançar*.
7. Clique em *Concluir*.
8. Clique em Test Data Source… (Testar Fonte de Dados). Você deve conseguir estabelecer uma conexão. Clique em *OK* até sair.

Instalando o Crystal Server para Oracle

Instale o Crystal Reports Server 11 com as seguintes opções selecionadas.

- Execute a instalação do servidor

- Instalar um novo BusinessObjects Enterprise System com *Install MSDE or use existing local SQL Server* (Instalar MSDE ou usar Servidor SQL local existente).

NOTA: O Crystal Server e o MS SQL Server 2000 devem residir na mesma máquina.

- IIS ASP.NET.

NOTA: Se você não tiver instalado o IIS e o ASP.NET usando o *Painel de Controle > Adicionar Remover Programas > Adicionar ou Remover Componentes do Windows*, o IIS ASP.NET ficará esmaecido.

- Você será solicitado a especificar o Modo de Autenticação. Selecione *Autenticação do Servidor SQL*.

O Crystal Reports tem suporte para acesso direito a bancos de dados do Oracle 9. Esse tipo de acesso é fornecido pelo arquivo de tradução crdb_oracle.dll. Esse arquivo se comunica com o driver do banco de dados do Oracle 9, que funciona diretamente com bancos de dados do Oracle e clientes, recuperando os dados de que você precisa no relatório.

NOTA: Para que o Crystal Reports use bancos de dados do Oracle 9, o software do cliente do Oracle deve ser instalado no sistema, e o local do cliente do Oracle deve estar na variável de ambiente PATH.

Instalando e configurando o software cliente do Oracle 9i

Ao instalar o cliente do Oracle 9i:

- Aceite o local de instalação padrão
- Não – para Perform Typical Configuration (Realizar Configuração Típica)
- Não – para Serviço de Diretório
- Selecione *Local*
- Nome do serviço TNS: ESEC
- Usuário (opcional): esecrpt

Após a instalação, crie uma configuração de nome de serviço de rede local.

Criando uma configuração de nome de serviço de rede (Configurando o driver nativo do Oracle)

1. Selecione *Oracle-OraHome92 > Configuration and Migration Tools > Net Manager*.
2. No painel de navegação, expanda Local e realce Service Naming (Nome de Serviço).
3. Clique no sinal de mais à esquerda para adicionar um nome de serviço.

4. Na janela Service Name (Nome de Serviço), digite um nome de serviço de rede.
   - Digite SENTINELDB

   Clique em *Avançar*.
5. Na janela Select Protocols (Selecionar Protocolos), selecione o padrão:
   - TCP/IP (Protocolo da Internet)

   Clique em *Avançar*.
6. Para o nome do host e o número da porta:
   - Digite o nome do host ou o endereço IP da máquina em que reside o banco de dados
   - Selecione a Porta Oracle (padrão 1521 durante a instalação)

   Clique em *Avançar*.
7. Para identificar o banco de dados ou o serviço:
   - Selecione (*Oracle8i ou posterior*), digite o nome do serviço (este é o nome da instância do Oracle).
   - Para o tipo de conexão, selecione *Database Default* (Banco de Dados Padrão).

   Clique em *Avançar*.
8. Na janela de teste, clique em *Testar*... Clique em *Avançar*. O teste pode falhar porque ele usa um ID de banco de dados e uma senha.
9. Se o teste falhar, execute este procedimento:
   - Na janela Connecting (Conectando), clique em *Change Login* (Mudar Login).
   - Digite o ID do Oracle do Sentinel (use esecrpt) e a senha. Clique em *OK*.

   Se o teste falhar:
   - Use o comando ping no Sentinel Server
   - Verifique se o nome do host do Sentinel Server está no arquivo de hosts no Crystal Reports Server. Esse arquivo se encontra em %SystemRoot%\system32\drivers\etc\.
10. Clique em *Concluir*.

Configuração para todas as autenticações e configurações

Mapeando o Crystal Reports para uso com o Sentinel

Os procedimentos a seguir são necessários para que o Crystal Server funcione com o Sentinel Control Center.

Configurando inetmgr

inetmgr

1. Copie o arquivo web.config de:

   ```
   C:\Arquivos de Programas\Business
      Objects\BusinessObjects Enterprise 11\Web Content
   ```

   para c:\Inetpub\wwwroot.

2. Inicie o Internet Service Manager clicando em *Iniciar* > *Executar*. Digite inetmgr e clique em *OK*.
3. *Expanda (computador local)* > *Web Sites* > *Default Web Site* > *businessobjects*.
4. Em *businessobjects*, clique o botão direito do mouse > *propriedades*.
5. Na guia *Virtual Directory* (Diretório Virtual), clique em *Configuration*... (Configuração).
6. Você deve ter os mapeamentos a seguir. Caso não os tenha, adicione-os. Se você for adicionar um mapeamento, não clique nos nós *businessobjects* ou *crystalreportsviewer11*.

Extensão	Executável
.csp	C:\Windows\Microsoft.NET\Framework\v1.1.4322\aspnet_isapi.dll
.cwr	C:\Windows\Microsoft.NET\Framework\v1.1.4322\aspnet_isapi.dll
.cri	C:\Windows\Microsoft.NET\Framework\v1.1.4322\aspnet_isapi.dll
.wis	C:\Arquivos de Programas\Business Objects\BusinessObjects Enterprise 11\win32_x86\cdzISAPI.dll

Clique em *OK* para fechar a janela.

7. Reinicie o IIS, expanda (computador local) > *Web Sites* > *Default Web Site*, realce *Default Web Site* (Web Site Padrão) e clique o botão direito em > *Iniciar*.

Aplicando patch do Crystal Reports para uso com o Sentinel

Para que os Crystal Reports sejam vistos na guia Análise do Sentinel Control Center, vários arquivos do Crystal Enterprise precisam ser atualizados para ficarem compatíveis com o browser embutido no Sentinel.

A tabela a seguir mostra esses arquivos e descreve para que cada um deles é usado.

Nome do arquivo	*Descrição*
`calendar.js` `calendar.html`	Exibe um calendário popup quando você seleciona uma data como parâmetro para um relatório.
`grouptree.html`	Exibe a mensagem Carregando... enquanto os relatórios são carregados.
`exportframe.html`	Exibe a janela em que você pode exportar um relatório para gravação ou impressão.
`exportIce.html`	Arquivo usado pelo Sentinel na exportação de um relatório para gravação ou impressão.
`GetInfoStore.asp`	Arquivo usado para consultar o Crystal Server
`GetReports.asp`	Arquivo usado pelo Sentinel Control Center para estabelecer uma conexão com o Crystal Server e exibir a lista de relatórios.

Nome do arquivo	***Descrição***
`GetReportURL.asp`	Arquivo usado para dar suporte a hiperlinks entre relatórios.
`helper_js.asp`	Um arquivo de chamadas usado por GetInfoStore.asp.

Patching Crystal Reports

1. No CD-ROM do Service Pack do Sentinel, vá para \content\reports\patch e copie todos os arquivos *.html e *.js para o local do arquivo do visualizador. O padrão é:

```
C:\Arquivos de Programas\Business
   Objects\BusinessObjects Enterprise 11\Web
   Content\Enterprise11\viewer\en
```

2. No CD-ROM do Service Pack do Sentinel, vá para \content\reports\patch e copie todos os arquivos *.asp e *.js para:

```
C:\inetpub\wwwroot
```

NOTA: A pasta da Web pode estar em uma unidade ou um local diferente da especificação acima.

Gabaritos do Crystal Report

Os gabaritos do Crystal Report são publicados usando o Crystal Publishing Wizard.

Pode-se fazer o download do conjunto mais recente de gabaritos de relatório no portal do cliente em http://esecurity.custhelp.com/.

NOTA: A lista de ataques por relatório CVE é uma interseção de assinaturas de ataque de vulnerabilidades alimentadas e exploradas do Advisor.

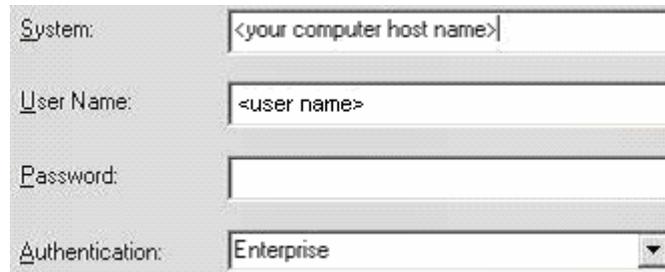
NOTA: Para executar um dos relatórios 10 Primeiros, alguns resumos agregados devem ser habilitados e o EventFileRedirectService (no processo DAS_Binary) deve ser ativado. Para obter informações sobre como habilitar os resumos agregados e ativar EventFileRedirectService, consulte a seção Habilitando os relatórios 10 Primeiros do Sentinel.

Publicando gabaritos de relatório usando o Crystal Publishing Wizard

Publicando gabaritos do Crystal Reports

NOTA: Se você quiser publicar os gabaritos de relatórios novamente, exclua os gabaritos importados anteriormente.

1. Clique em *Iniciar* > *Todos os Programas* > *BusinessObjects 11* > *Crystal Reports Server* > *Assistente de Publicação*.
2. Clique em *Avançar*.
3. Efetue login. Sistema deve ser o nome do seu computador host e Autenticação deve ser Enterprise. O nome do usuário pode ser Administrador. Por questão de segurança, recomenda-se enfaticamente criar um novo usuário diferente de Administrador. Digite sua senha e clique em *Avançar*.

NOTA: Relatórios publicados no usuário Administrador podem ser acessados por todos os usuários.

System: <your computer host name>
User Name: <user name>
Password:
Authentication: Enterprise

4. Clique em *Adicionar Pasta*.
5. Selecione *Incluir Subpasta*. Vá para o CD-ROM do Service Pack do Sentinel e navegue para:

   Para o Crystal Reports (usuários do MS SQL):

   ```
   \content\reports\Crystal_v11\SQL-Server
   ```

   Para o Crystal Reports (usuários do Oracle):

   ```
   \content\reports\Crystal_v11\Oracle
   ```

   Clique em *OK*.
6. Clique em *Avançar*.
7. Na janela Especificar Localização, clique em *Nova Pasta* (canto superior direito) e crie uma pasta chamada *Sentinel_Reports*. Clique em *Avançar*.

8. Selecione:
   - *Duplicar hierarquia de pasta*;
   - Clique na seta para baixo e selecione <*não incluir*>.

   Clique em *Avançar*;
9. Na janela Confirm Location (Confirmar Local), clique em *Avançar*.

10. Na janela Especificar Categorias:
    - selecione um nome de categoria (como sentinel);
    - realce o nome e clique no botão +;

NOTA: Somente o primeiro relatório será exibido na categoria depois que você clicar em Avançar.

    - clique em *Avançar*.
11. Na janela Especificar Programação, clique em *Permitir que usuários atualizem o objeto* (essa deve ser a opção padrão). Clique em *Avançar*.
12. Na janela Especificar Atualização do Repositório, clique em *Habilitar Tudo* para habilitar a atualização do repositório. Clique em *Avançar*.
13. Na janela Specify Keep Saved Data (Especificar Manutenção dos Dados Gravados), clique em *Ativar Tudo* para manter os dados gravados quando publicar relatórios. Clique em *Avançar*.
14. Na janela Mudar Valores Padrão, clique em *Publicar relatórios sem modificar propriedades* (essa deve ser a opção padrão). Clique em *Avançar*.
15. Clique em *Avançar* para adicionar seus objetos.
16. Clique em *Avançar*.
17. Uma lista publicada será exibida; clique em *Concluir*.

Quando os gabaritos do Sentinel para Crystal Reports são publicados no Crystal Enterprise Server, os gabaritos devem residir no diretório *Sentinel_Reports*.

Definindo uma conta de 'Usuário Nomeado'

A chave de licença fornecida com o Crystal Server é uma chave de conta 'Usuário Nomeado'. A conta Guest foi mudada de 'Usuário Simultâneo' para 'Usuário Nomeado'.

Definindo a conta Guest como 'Usuário Nomeado'

1. Clique em *Iniciar > Todos os Programas > BusinessObjects 11 > Crystal Reports Server > .NET Administration Launchpad*.
2. Clique em *Central Management Console*.
3. O nome do sistema deve ser o nome do computador do host. O tipo de autenticação deve ser Enterprise. Caso contrário, escolha *Enterprise*.
4. Clique em *Log On* (Fazer conexão).
5. No painel Organizar, clique em *Usuários*.
6. Clique em *Guest*.
7. Mude o tipo de conexão de *Usuário Simultâneo* para *Usuário Nomeado*.
8. Clique em *Update* (Atualizar).
9. Faça logoff e feche a janela ou vá para a seção *Configurando o .NET Administration Launchpad*.

Configurando o .NET Administration Launchpad

Este procedimento discute como configurar o .NET Administration Launchpad para permitir que você veja e modifique relatórios.

Configurando o .NET Administration Launchpad

1. Se ainda não tiver feito isso, inicie o .NET Administration Launchpad (clique em *Iniciar > Todos os Programas > BusinessObjects 11 > Crystal Reports Server > .NET Administration Launchpad*).
2. Clique em *Central Management Console*.

   O nome do sistema deve ser o nome do computador do host. O tipo de autenticação deve ser Enterprise. Caso contrário, escolha *Enterprise*.
3. Digite o nome do usuário e a senha e clique em *Log On*.
4. No painel Organizar, clique em *Pastas*.
5. Clique em *Sentinel_Reports*;
6. Selecione *Tudo*.
7. Clique na guia *Direitos*.
8. Para Everyone (Todos), no menu suspenso à direita de Access Level (Nível de Acesso), selecione *View on Demand* (Ver por Demanda). Clique em *Update* (Atualizar).

   NOTA: Ao mudar o nível de acesso de *(Inherited Rights)* (Direitos Herdados) para *View on Demand* (Ver por Demanda), o processo de atualização congela. Aguarde aproximadamente trinta segundos. O nível de acesso será atualizado.
9. Efetue logoff e feche a janela.

Testando a conexão do servidor Web com o banco de dados

Testando a conexão do servidor Web com o banco de dados

1. Se ainda não tiver feito isso, inicie o .NET Administration Launchpad (*Iniciar > Todos os Programas > BusinessObjects 11 > Crystal Reports Server > .NET Administration Launchpad*).
2. Clique em *Central Management Console*.
3. Digite Administrator como o nome do usuário. Digite a senha (por padrão, este campo estará vazio). Clique em *Log On* (Fazer conexão).
4. Navegue até *Pastas Públicas > Sentinel_Reports > Eventos Internos*.
5. Selecione *Column Display Details* (Detalhes de Exibição de Coluna).
6. Clique em *Visualizar*.
7. Dependendo do sistema, faça login como esecrpt ou como o usuário do Relatório do Sentinel.
8. No menu suspenso do campo de classificação, selecione *Tag*.
9. Clique em *OK*. Um relatório deve ser exibido.

Testando a conectividade com o servidor Web

Testando a conectividade com o servidor Web

1. Vá para outra máquina na mesma rede que o servidor Web.
2. Digite

```
http://<nome DNS ou endereço IP do servidor
   Web>/businessobjects/enterprise11/WebTools/adminlau
   nch/default.aspx
```

3. Você deve obter uma página Web do Crystal BusinessObjects.

Habilitando os relatórios 10 Primeiros do Sentinel

Para habilitar os relatórios 10 Primeiros do Sentinel, é necessário:

- Ativar a agregação;
- Habilitar o EventFileRedirectService;

Ativando a agregação

1. Inicie o Gerenciador de Dados do Sentinel.
2. Efetue login.
3. Clique na guia *Relatando Dados*.
4. Habilite estes resumos:
   - EventDestSummary
   - EventSevSummary
   - EventSrcSummary

   Clique nos botões '*Inativo*' na coluna Status até que mudem para '*Ativo*'.

Summary Name	Time	Attributes	Source	Status
EventDestSummary	1 hour	CUST_ID,RSRC_ID ...	TransformedEvent	Active
EventSevDestTxnmy...	1 hour	CUST_ID,DEST_EV ...	TransformedEvent	InActive
EventSevDestEvtSu...	1 hour	CUST_ID,DEST_EV ...	TransformedEvent	InActive
EventSevDestPortSu...	1 hour	SEV,DEST_PORT,C ...	TransformedEvent	InActive
EventSevSummary	1 hour	CUST_ID,SEV,EVT ...	TransformedEvent	Active
EventSrcSummary	1 hour	CUST_ID,RSRC_ID ...	TransformedEvent	Active

Habilitando o EventFileRedirectService

1. Na máquina DAS, usando o editor de texto, abra:

   Para UNIX:

   ```
   $ESEC_HOME/sentinel/config/das_binary.xml
   ```

   Para Windows:

   ```
   %ESEC_HOME%\sentinel\config\das_binary.xml
   ```

2. Para o EventFileRedirectService, mude o status para "on" (ativado):

   ```
   <property name="status">on</property>
   ```

3. Reinicie o componente DAS, executando este procedimento:

   No Windows:

   ```
   Use o Gerenciador de Serviços para parar e, depois,
      iniciar o serviço "sentinel".
   ```

   No Solaris:

   ```
   $ESEC_HOME/sentinel/scripts/sentinel.sh stop
   ```

   ```
   Verifique se todos os processos do Sentinel Server
      nesta máquina pararam usando o comando 'ps –ef |
      grep $ESEC_USER'. Se alguns processos do Sentinel
      Server ainda estiverem em execução, elimine-os
      usando o comando kill.
   ```

   ```
   $ESEC_HOME/sentinel/scripts/sentinel.sh start
   ```

Maximizando a geração de relatórios de eventos

Dependendo do número de eventos que o Crystal estiver consultando, você poderá receber um erro sobre o tempo máximo de processamento ou o limite máximo de registros. Para definir o servidor para processar um número maior ou ilimitado de relatórios, será necessário reconfigurar o Crystal Page Server. Há dois métodos para fazer isso: usando o Central Configuration Manager ou usando a página da Web Crystal.

Reconfigurando o Crystal Page Server via Central Configuration Manager

1. Clique em *Iniciar* > *Todos os Programas* > *BusinessObjects 11* > *Crystal Reports Server* > *Central Configuration Manager*.
2. Clique o botão direito em *Crystal Reports Page Server* e selecione *Parar*.
3. Clique o botão direito em *Crystal Reports Page Server* e selecione *Propriedades*.
4. No campo Comando na guia Propriedades, no fim da linha do comando, adicione -maxDBResultRecords <valor maior do que 20.000 ou 0 para desabilitar o limite padrão>
5. Reinicie o Crystal Page Server.

Reconfigurando o Crystal Page Server via página da Web Crystal

1. Abra um browser e digite este url:

   ```
   http://<nome DNS ou endereço IP do servidor
      Web>/businessobjects/enterprise11/WebTools/adminlau
      nch/default.aspx
   ```

2. Clique em *Central Management Console*.
3. O nome do sistema deve ser o nome do computador do host. O tipo de autenticação deve ser Enterprise. Caso contrário, escolha Enterprise.
4. Digite o nome do usuário e a senha e clique em *Log On*.
5. Clique em *Servers* (Servidores).
6. Clique em *<nome do servidor>.pageserver*.
7. Em 'Registros do Banco de Dados para Ler ao Visualizar ou Atualizar um Relatório', selecione *Registros ilimitados*.

8. Clique em *Apply*.
9. Será exibido um prompt para reiniciar o servidor de página; clique em *OK*.
10. Talvez seja preciso fornecer um nome de logon e uma senha para acessar o gerenciador do serviço do sistema operacional.

Configurando o Sentinel para integração com o Crystal Enterprise Server

Depois de instalado o Crystal Enterprise Server, o Sentinel Control Center pode ser configurado para acessar os relatórios diretamente por meio do Sentinel Control Center.

Configurando o Sentinel para integração com o Crystal Enterprise Server

1. Efetue login no Centro de Controle do Sentinel como um usuário com privilégios para a guia Admin;
2. Na guia Admin, selecione *Configuração de Relatórios*.
3. No campo URL de Análise, digite o seguinte:

```
http://<nome_do_host_ou_IP_do_servidor_web>/GetReports
   .asp?APS=<nome_do_host>&user=Guest&password=&tab=An
   alysis
```

NOTA: <nome_do_host_ou_IP_do_servidor_web> deve ser substituído pelo endereço IP ou o nome do host do Crystal Enterprise Server.

NOTA: O URL acima não funcionará corretamente se o APS estiver definido como o endereço IP. Ele deve ser o nome do host do Crystal Server.

4. Clique em *Atualizar* ao lado do campo URL de Análise.
5. Se o Advisor estiver instalado, digite o seguinte no campo URL de Análise:

```
http://<nome_do_host_ou_IP_do_servidor_web>/GetReports
   .asp?APS=<nome_do_host>&user=Guest&password=&tab=Ad
   visor
```

NOTA: <nome_do_host_ou_IP_do_servidor_web> deve ser substituído pelo endereço IP ou o nome do host do Crystal Enterprise Server.

NOTA: O URL acima não funcionará corretamente se o APS estiver definido como o endereço IP. Ele deve ser o nome do host do Crystal Server.

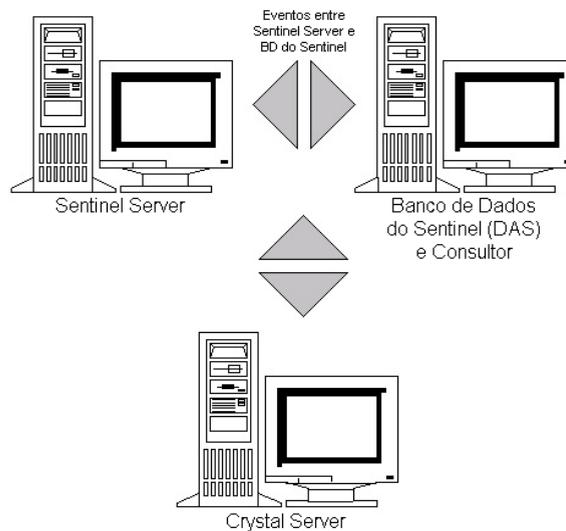
6. Clique em *Atualizar* ao lado do campo URL de Consultor.
7. Clique em *Gravar*.
8. Efetue logout e login novamente no Sentinel Control Center. As árvores do Crystal Report nas guias Análise e Consultor (se o Advisor estiver instalado) devem agora aparecer na janela Navegador.

10 Crystal Reports para Linux

NOTA: O termo Agente é sinônimo de Coletor. De agora em diante, Agentes serão referidos como Coletores.

O Crystal BusinessObjects Enterprise™ 11 é uma das ferramentas de geração de relatórios que se integram ao Sentinel.

Este capítulo descreve a configuração da instalação do Crystal Reports Server do Sentinel no Linux. A instalação deve ser feita na ordem apresentada.

- Pré-instalação e instalação do Crystal BusinessObjects Enterprise™ 11;
- Aplicação do patch do Crystal Reports;
- Publicação (importação) de Crystal Reports;
- Definição de uma conta de 'Usuário Nomeado';
- Teste de conectividade com o servidor Web;
- Habilitação dos 10 Relatórios Principais (opcional);
- Maximização de Relatórios de Eventos (recomendado);
- Configuração do Sentinel para o Crystal Enterprise Server.

Usando Crystal Reports

Para obter informações sobre como usar o Crystal Reports para geração de relatórios do Sentinel, consulte *Crystal Reports Documentation* e o *Guia do Usuário do Sentinel*.

Configuração

- Versões para Linux:
  - SuSE Linux Enterprise Server 9 (SLES 9);
  - Red Hat Enterprise Linux 3 Atualização 5 ES (x86);
- BusinessObjects Enterprise XI Server instalado;
- Para Oracle - Oracle 9i Client Release 2 (9.2.0.1.0).

Instalação

Pré-instalando o Crystal BusinessObjects Enterprise™ 11

Pré-instalando o Crystal BusinessObjects Enterprise

1. Se o banco de dados do Sentinel não estiver na mesma máquina que o Crystal Server, você deverá instalar o software Oracle Client na máquina do Crystal Server. Esta etapa adicional não será necessária se o banco de dados do Sentinel estiver na mesma máquina do Crystal Server, pois nesse caso o software Oracle necessário já está instalado com o software do banco de dados Oracle exigido pelo banco de dados do Sentinel.
2. Efetue login na máquina do Crystal Server como usuário Root.
3. Crie o grupo bobje:

   ```
   groupadd bobje
   ```

4. Crie um usuário do Crystal (o diretório deste exemplo é o "/export/home/crystal", você pode mudá-lo se necessário; a parte "/export/home" do caminho já deve existir):

   ```
   useradd –g bobje –s /bin/bash –d /export/home/crystal
      –m crystal
   ```

5. Crie um diretório para o software de relatórios Crystal:

   ```
   mkdir –p /opt/crystal_xi
   ```

6. Mude a propriedade do diretório do software de Crystal (recursivamente) para crystal/bobje:

   ```
   chown -R crystal:bobje /opt/crystal_xi
   ```

7. Mude para o usuário do Crystal:

   ```
   su - crystal
   ```

8. A variável de ambiente ORACLE_HOME deve ser definida no ambiente do usuário do Crystal. Para fazer isso, modifique o script de login do usuário do Crystal para definir a variável de ambiente ORACLE_HOME para a base do software Oracle. Por exemplo, se o shell do usuário do Crystal for um bash e o software Oracle estiver instalado no diretório /opt/oracle/product/9.2, abra o arquivo ~crystal/.bash_profile e adicione a seguinte linha ao final do arquivo:

   ```
   export ORACLE_HOME=/opt/oracle/product/9.2
   ```

9. A variável de ambiente LD_LIBRARY_PATH no ambiente do usuário do Crystal deve conter o caminho para as bibliotecas do software Oracle. A variável de ambiente LD_LIBRARY_PATH no ambiente do usuário do Crystal deve conter o caminho para as bibliotecas do software Oracle. Por exemplo, se o shell do usuário do Crystal for um bash, abra o arquivo ~crystal/.bash_profile e adicione a seguinte linha ao final do arquivo (abaixo da variável de ambiente ORACLE_HOME definida):

   ```
   export
      LD_LIBRARY_PATH=$ORACLE_HOME/lib:$LD_LIBRARY_PATH
   ```

10. Deve ser adicionada uma entrada ao arquivo tnsnames.ora do Oracle com o Nome do Serviço "esecuritydb", que aponta para o banco de dados do Sentinel. Para fazer isso na máquina do Crystal Server:

    a. Efetue login como usuário do Oracle;
    b. Mude os diretórios para $ORACLE_HOME/network/admin;
    c. Faça backup do arquivo tnsnames.ora;
    d. Abra o arquivo tnsnames.ora para edição;
    e. Se o banco de dados do Sentinel estiver na máquina do Crystal Server, já deve haver uma entrada no arquivo tnsnames.ora para o banco de dados do Sentinel. Por exemplo, se o banco de dados do Sentinel se chamar ESEC, existirá uma entrada semelhante a esta:

    ```
    ESEC =
    (DESCRIPTION =
     (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = dev-linux02)(PORT
       = 1521))
      )
      (CONNECT_DATA =
      (SID = ESEC)
      )
    )
    ```

    f. Se o banco de dados do Sentinel não estiver na máquina do Crystal Server, abra o arquivo arquivo tnsnames.ora na máquina do banco de dados do Sentinel para localizar a entrada descrita anteriormente.
    g. Faça uma cópia de toda a entrada e cole-a no final do arquivo tnsnames.ora da máquina do Crystal Server. A parte da entrada do Nome do Serviço deve ser renomeada como "esecuritydb". Por exemplo, quando a entrada anterior é copiada e renomeada corretamente, fica da seguinte forma:

    ```
    esecuritydb =
    (DESCRIPTION =
     (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = dev-linux02)(PORT
       = 1521))
    ```

```
        )
        (CONNECT_DATA =
        (SID = ESEC)
        )
    )
```

h. Verifique se a parte da entrada HOST está correta (por exemplo, verifique se não está definida como localhost (host local) se o Crystal Server e o banco de dados do Sentinel estiverem em máquinas diferentes).
i. Grave as mudanças feitas no arquivo tnsnames.ora.
j. Execute o seguinte comando para verificar se o Nome do Serviço esecuritydb está configurado corretamente:

```
tnsping esecuritydb
```

k. Se o comando for executado corretamente, você receberá uma mensagem que informa que a conexão está OK.

Instalando o Crystal BusinessObjects Enterprise™ 11

Instalando o Crystal BusinessObjects Enterprise

1. Efetue login como usuário do Crystal.
2. Mude os diretórios no DISK_1 do instalador do Crystal.
3. Execute:

```
./install
```

4. Selecione o Idioma: *Inglês*.
5. Selecione *Nova Instalação*.
6. Aceite o Contrato de Licença.
7. Digite o Código do Produto.
8. Digite o diretório de instalação:

```
/opt/crystal_xi
```

9. Selecione: *Instalação do usuário.*
10. Selecione: *Nova Instalação.*
11. Selecione: *Instalar MySQL.*
12. Digite informações de configuração do MySQL:
    a. Use a porta padrão 3306
    b. Senha do administrador
13. Digite mais informações de configuração do MySQL:
    a. Nome do BD padrão: BOE11
    b. ID de usuário: mysqladm
    c. Senha
14. Digite mais informações de configuração do MySQL:
    a. Servidor de Nomes Local: <nome de host da máquina local>
    b. Número da Porta CMS Padrão: 6400.

15. Selecione: *Instalar Tomcat*;
16. Digite informações de configuração do Tomcat:
    a. Porta padrão de solicitações HTTP de recebimento: 8080
    b. Porta padrão de solicitações JSP de redirecionamento: 8443
    c. Porta padrão hook de encerramento: 8005
17. Pressione *Enter* para iniciar a instalação.

Aplicando patch do Crystal Reports para uso com o Sentinel

Para que os Crystal Reports sejam vistos na guia Análise do Sentinel Control Center, vários arquivos do Crystal Enterprise precisam ser atualizados para ficarem compatíveis com o browser embutido no Sentinel.

A tabela a seguir mostra esses arquivos e descreve para que cada um deles é usado.

Nome do arquivo	***Descrição***

`calendar.js`
 	
`calendar.html`
	Exibe um calendário popup quando você seleciona uma data como parâmetro para um relatório.

`grouptree.html`	Exibe a mensagem Carregando... enquanto os relatórios são carregados.
`exportframe.html`	Exibe a janela em que você pode exportar um relatório para gravação ou impressão.
`exportIce.html`	Arquivo usado pelo Sentinel na exportação de um relatório para gravação ou impressão.
`GetReports.jsp`	Arquivo usado pelo Sentinel Control Center para estabelecer uma conexão com o Crystal Server e exibir a lista de relatórios.

Aplicando patch do Crystal Reports

1. AGORA DISPONÍVEL APENAS NO SERVICE PACK. No CD-ROM do Service Pack do Sentinel, vá para \content\reports\patch e copie todos os arquivos *.html e *.js na localização do arquivo do viewer. O padrão é:

   ```
   /opt/crystal_xi/bobje/webcontent/enterprise11/viewer/en/
   ```

2. No CD-ROM do Service Pack do Sentinel, vá para \content\reports\patch e copie todos os arquivos *.jsp em:

   `/opt/crystal_xi/bobje/tomcat/webapps/`**`esec-script`**`/`

   NOTA: Crie uma pasta chamada **esec-script**.

   ```
   Copie todos os arquivos *.jar
   ```

De:

```
/opt/crystal_xi/bobje/tomcat/webapps/jsfadmin/WEB-
   INF/lib/
```

Para:

```
   /opt/crystal_xi/bobje/tomcat/webapps/esec-
   script/WEB-INF/lib
```

NOTA: Crie uma estrutura de pastas **WEB-INF/lib**.

Publicando gabaritos de Crystal Reports

Estes gabaritos de relatório são criados pela Novell para uso nas guias Análise e Consultor do Sentinel Control Center.

Existem dois métodos de publicação de relatórios:

- Assistente de Publicação de Crystal Reports;
- Console de Gerenciamento Central do Crystal Reports.

Também são fornecidos exemplos dos relatórios no formato pdf.

NOTA: A lista de ataques por relatório CVE é uma interseção de assinaturas de ataque de vulnerabilidades alimentadas e exploradas do Advisor.

NOTA: Para os 10 relatórios principais serem executados, a agregação deve ser habilitada e o EventFileRedirectService no DAS_Binary.xml deve ser ativado. Para obter informações sobre como habilitar uma agregação, consulte o *Capítulo 10 do Guia do usuário do Sentinel, Gerenciador de dados do Sentinel*, seção *Guia Relatando dados, ou a seção* Enabling Sentinel Top 10 Reports.

Publicando gabaritos de relatórios – Assistente de Publicação de Crystal Reports

NOTA: Uma plataforma Windows é obrigatória para a execução do Assistente de Publicação de Relatórios Crystal.

Importando gabaritos de Crystal Reports

NOTA: Se você importar (publicar) seus Gabaritos de Relatórios outra vez, apague a importação anterior dos Gabaritos de Relatórios.

1. Clique em *Iniciar > Todos os Programas > BusinessObjects 11 > Crystal Reports Server > Assistente de Publicação.*
2. Clique em *Avançar*.
3. Efetue login. Sistema deve ser o nome do seu computador host e Autenticação deve ser Enterprise. O Nome de Usuário pode ser o Administrador. Por segurança, você deve usar um usuário que não seja o Administrador. Digite sua senha e clique em *Avançar*.

NOTA: Relatórios publicados no usuário Administrador podem ser acessados por todos os usuários.

4. Clique em *Adicionar Pasta*.
5. Clique em *Incluir Subpasta*. Vá para o CD-ROM do Service Pack do Sentinel e navegue para:

   ```
   content\reports\Crystal_v11\Oracle
   ```

   Clique em *OK*.
6. Clique em *Avançar*.
7. Na janela Especificar Localização, clique em *Nova Pasta* (canto superior direito) e crie uma pasta chamada *eSecurity_Reports*. Clique em *Avançar*.

8. Selecione:
   - *Duplicar hierarquia de pasta*;
   - Clique na seta para baixo e selecione <*não incluir*>.

   Clique em *Avançar*;
9. Na janela Confirmar Localização, clique em *Avançar*.
10. Na janela Especificar Categorias:
    - Selecione um nome de categoria (como sentinel);
    - Realce o nome e clique no botão +;

NOTA: Somente o primeiro relatório será exibido na categoria depois que você clicar em Avançar.

- Clique em *Avançar*.

11. Na janela Especificar Programação, clique em *Permitir que usuários atualizem o objeto* (essa deve ser a opção padrão). Clique em *Avançar*.
12. Na janela Especificar Atualização do Repositório, clique em *Habilitar Tudo* para habilitar a atualização do repositório. Clique em *Avançar*.
13. Na janela Especificar Dados Gravados Mantidos, clique em *Habilitar Tudo* para manter os dados gravados ao publicar relatórios. Clique em *Avançar*.
14. Na janela Mudar Valores Padrão, clique em *Publicar relatórios sem modificar propriedades* (essa deve ser a opção padrão). Clique em *Avançar*.
15. Clique em *Avançar* para adicionar seus objetos.
16. Clique em *Avançar*.
17. Clique em *Concluir*.

Quando os gabaritos do Sentinel para Crystal Reports são publicados no Crystal Enterprise Server, eles devem ficar no diretório *eSecurity_Reports*.

Publicando gabaritos de relatório – Console de Gerenciamento Central

Quando são publicados com o Console de Gerenciamento Central, os relatórios não podem ser publicados em lote, como quando se usa o Assistente para Publicação do Windows.

Importação de gabaritos de Crystal Reports

1. Abra um browser e digite este url:

```
http://<nome_do_host_ou_IP_do_servidor_web>:<porta_padrão_servidor_web_8080>/businessobjects/enterprise11/adminlaunch
```

2. Clique em *Console de Gerenciamento Central*.
3. Efetue login no Crystal Server.
4. No painel *Organizar*, clique em *Pastas*.
5. No canto superior direito, clique em *Nova Pasta...*
6. Crie uma pasta denominada *eSecurity_Reports*. Clique em *OK*.
7. Clique em *eSecurity_Reports*.
8. Clique na guia Subpastas e crie estas subpastas:
   - Vulnerabilidade do Consultor
   - Gerenciamento de Incidentes
   - Eventos Internos
   - Eventos de Segurança
   - 10 Principais
9. Clique em *Home*.

10. Clique em *Objetos*.
11. Clique em *Novo Objeto*.
12. À esquerda da página, realce o *Relatório*.
13. Clique no botão Procurar e procure o CD do Service Pack do Sentinel:

    ```
    content\reports\Crystal_v11\Oracle
    ```

    Escolha uma pasta e selecione um relatório.
14. Realce *eSecurity_Reports* e clique em *Mostrar Subpastas*.
15. Selecione a pasta apropriada para o relatório e clique em *Mostrar Subpastas*.
16. Clique em *OK*.
17. Clique em *Atualizar*.
18. Clique na guia *Relatórios* e continue a adicionar relatórios.
19. Para adicionar os relatórios restantes a outra pasta, clique em *Pastas*, no canto superior esquerdo, e repita as etapas 14 a 17.

Usando o servidor Web Crystal XI

O Crystal Server XI no Linux instala um servidor Web com o qual você pode executar tarefas administrativas além de publicar e ver relatórios.

O portal administrativo é acessado via browser no seguinte URL:

```
http://<nome_do_host_ou_IP_do_servidor_web>:<porta_padrão
   _servidor_web_8080>/businessobjects/enterprise11/admin
   launch
```

O portal não-administrativo, ou de uso geral, é acessado via browser no seguinte URL:

```
http://<nome_do_host_ou_IP_do_servidor_web>:<porta_padrão
   _servidor_web_8080>/businessobjects/enterprise11
```

Testando a conectividade com o servidor Web

Testando a conectividade com o servidor Web

1. Vá para outra máquina na mesma rede que o servidor Web.
2. Digite

    ```
    http://<nome_do_host_ou_IP_do_servidor_web>:<porta_pad
       rão_servidor_web_8080>/businessobjects/enterprise11
       /adminlaunch
    ```

3. Você deve obter uma página Web do Crystal BusinessObjects.

Definindo uma conta de 'Usuário Nomeado'

A chave de licença fornecida com o Crystal Server é uma chave de conta 'Usuário Nomeado'. A conta Guest foi mudada de 'Usuário Simultâneo' para 'Usuário Nomeado'.

Definindo a conta Guest como 'Usuário Nomeado'

1. Abra um browser e digite este url:

```
http://<nome_do_host_ou_IP_do_servidor_web>:<porta_pad
   rão_servidor_web_8080>/businessobjects/enterprise11
   /adminlaunch
```

2. Clique em *Console de Gerenciamento Central*.
3. O nome do sistema deve ser o nome do computador do host. O tipo de autenticação deve ser Enterprise. Caso contrário, escolha Enterprise.
4. No painel Organizar, clique em *Usuários*.
5. Clique em *Guest*.
6. Mude o tipo de conexão de *Usuário Simultâneo* para *Usuário Nomeado*.
7. Clique em *Atualizar*.
8. Efetue logoff e feche a janela.

Configurando relatórios

Este procedimento descreve como configurar o Administration Launchpad para permitir que você veja e modifique relatórios.

Configurando o Administration Launchpad

1. Abra um browser e digite este url:

```
http://<nome_do_host_ou_IP_do_servidor_web>:<porta_pad
   rão_servidor_web_8080>/businessobjects/enterprise11
   /adminlaunch
```

2. Clique em *Console de Gerenciamento Central.*
3. O nome do sistema deve ser o nome do computador do host. O tipo de autenticação deve ser Enterprise. Caso contrário, escolha *Enterprise*.
4. Digite o nome do usuário e a senha e clique em *Logon*.
5. No painel Organizar, clique em *Pastas*.
6. Clique em *eSecurity_Reports*.
7. Selecione *Tudo*.
8. Clique na guia Direitos.
9. Em Todos, no menu suspenso à direita, selecione *Ver por Demanda*. Clique em *Atualizar*.
10. Efetue logoff e feche a janela.

Habilitando os relatórios 10 Primeiros do Sentinel

Para habilitar os relatórios 10 Primeiros do Sentinel, é necessário:

- Ativar a agregação;
- Habilitar o EventFileRedirectService.

Ativando a agregação

1. Inicie o Gerenciador de Dados do Sentinel.
2. Efetue login.
3. Clique na guia *Relatando Dados*.
4. Habilite estes resumos:
   - EventDestSummary
   - EventSevSummary
   - EventSrcSummary

   Clique nos botões 'Inativo' na coluna Status até que mudem para 'Ativo'.

Summary Name	Time	Attributes	Source	Status
EventDestSummary	1 hour	CUST_ID.RSRC_ID ...	TransformedEvent	Active
EventSevDestTxnmy...	1 hour	CUST_ID.DEST_EV ...	TransformedEvent	InActive
EventSevDestEvtSu...	1 hour	CUST_ID.DEST_EV ...	TransformedEvent	InActive
EventSevDestPortSu...	1 hour	SEV.DEST_PORT.C ...	TransformedEvent	InActive
EventSevSummary	1 hour	CUST_ID.SEV.EVT ...	TransformedEvent	Active
EventSrcSummary	1 hour	CUST_ID.RSRC_ID ...	TransformedEvent	Active

Habilitando o EventFileRedirectService

1. Na máquina DAS, usando o editor de texto, abra:

   ```
   $ESEC_HOME/sentinel/config/das_binary.xml
   ```

2. Para o EventFileRedirectService, mude o status para "on" (ativado):

   ```
   <property name="status">on</property>
   ```

3. Reinicie o processo DAS_Binary. Para fazer isso, use o Sentinel Control Center ou reinicialize a máquina.

   Usando o Sentinel Control Center:

   - Efetue login no Sentinel Control Center como um usuário com direitos de administrador. Esse usuário deve ter as seguintes permissões de "Telas de Servidor":
     - Ver Servidores
     - Controlar Servidores
   - Na guia Admin, abra uma tela de servidor para ver todos os processos do Sentinel Server.
   - Clique o botão direito do mouse no processo *DAS_Binary* e selecione *Reiniciar*.
   - A conta "Início" desse processo aumentará em uma unidade se o processo for reiniciado com êxito.

Maximizando a geração de relatórios de eventos

Dependendo do número de eventos que o Crystal estiver consultando, você poderá receber um erro sobre o tempo máximo de processamento ou o limite máximo de registros. Para definir o servidor para processar um número maior ou ilimitado de relatórios, será necessário reconfigurar o Crystal Page Server.

Reconfigurando o Crystal Page Server

1. Abra um browser e digite este url:

```
http://<nome_do_host_ou_IP_do_servidor_web>:<porta_pad
   rão_servidor_web_8080>/businessobjects/enterprise11
   /adminlaunch
```

2. Clique em *Console de Gerenciamento Central*.
3. O nome do sistema deve ser o nome do computador do host. O tipo de autenticação deve ser Enterprise. Caso contrário, escolha Enterprise.
4. Digite o nome do usuário e a senha e clique em *Logon*.
5. Clique em *Servidores*.
6. Clique em *<nome do servidor>.pageserver*.
7. Em *Registros do Banco de Dados para Ler ao Visualizar ou Atualizar um Relatório*, selecione *Registros ilimitados*.
8. Clique em *Aplicar*.
9. Será exibido um prompt para reiniciar o servidor de página, clique em *OK*.
10. Talvez seja preciso fornecer um nome de logon e uma senha para acessar o gerenciador do serviço do sistema operacional.

Configurando o Sentinel para o Crystal Enterprise Server

Depois de instalado o Crystal Enterprise, o Sentinel Control Center precisa ter os URLs para os relatórios de análise.

Configurando o Sentinel para o Crystal Enterprise Server

1. Efetue login no Sentinel Control Center como um usuário com privilégios para a guia Admin.
2. Na guia Admin, selecione *Configuração de Relatórios*.
3. No campo URL de Análise, digite o seguinte:

```
http://<nome_do_host_ou_IP_do_servidor_web>:<porta_pad
   rão_servidor_web_8080>/esec-
   script/GetReports.jsp?APS=<nome_do_host>&user=Guest
   &password=&tab=Analysis
```

NOTA: <nome_do_host_ou_IP_do_servidor_web> deve ser substituído pelo endereço IP ou o nome do host do Crystal Enterprise Server.

NOTA: O URL acima não funcionará corretamente se o APS estiver definido como o endereço IP. Ele precisa ser o nome do host.

NOTA: <porta_padrão_servidor_web_8080> deve ser substituído pela porta em que o servidor Web Crystal estiver escutando.

4. Clique em *Atualizar* ao lado do campo URL de Análise.
5. Se o Advisor estiver instalado, digite o seguinte no campo URL de Análise:

```
http://<nome_do_host_ou_IP_do_servidor_web>:<porta_pad
   rão_servidor_web_8080>/esec-
   script/GetReports.jsp?APS=<nome_do_host>&user=Guest
   &password=&tab=Advisor
```

NOTA: <nome_do_host_ou_IP_do_servidor_web> deve ser substituído pelo endereço IP ou o nome do host do Crystal Enterprise Server.

NOTA: O URL acima não funcionará corretamente se o APS estiver definido como o endereço IP. Ele precisa ser o nome do host.

NOTA: <porta_padrão_servidor_web_8080> deve ser substituído pela porta em que o servidor Web Crystal estiver escutando.

6. Clique em *Atualizar* ao lado do campo URL de Consultor.
7. Clique em *Gravar*.
8. Efetue logout e login novamente no Sentinel Control Center. As árvores do Crystal Report nas guias Análise e Consultor (se o Advisor estiver instalado) devem agora aparecer na janela Navegador.

Utilitários e solução de problemas

Iniciando o MySQL

Para verificar se o MySQL está em execução:

1. Efetue login como o usuário crystal.
2. cd /opt/crystal_xi/bobje
3. ./mysqlstartup.sh

Iniciando o Tomcat

Para verificar se o Tomcat está em execução:

1. Efetue login como o usuário crystal.
2. cd /opt/crystal_xi/bobje
3. ./tomcatstartup.sh

Iniciando o Crystal Servers

Para verificar se o Crystal Servers está em execução:

1. Efetue login como o usuário crystal.
2. cd /opt/crystal_xi/bobje
3. ./startservers

Erro de nome de host Crystal

Erro de nome de host

1. Se receber este erro:

```
Aviso: ORB::BOA_init: pesquisa de nome de host
   retornou `localhost' (127.0.0.1)
```

```
Use a opção -OAhost para selecionar outro nome de host
```

   Verifique se o IP e o nome do host estão no arquivo /etc/hosts. Exemplo:

```
192.0.2.46  linuxCE02
```

Não é possível conectar-se ao CMS

Se o sistema relatar que não é possível conectar com o CMS, tente executar os comandos a seguir.

Solução de problemas de falha de conexão do CMS

1. Se o comando "netstat –an | grep 6400" não retornar um resultado, tente o seguinte:
   - Digite novamente as informações da conexão MySQL:

   a. Efetue login como o usuário crystal.
   b. cd /opt/crystal_xi/bobje
   c. ./cmsdbsetup.sh
   d. Pressione Enter quando for exibido "[<nome_do_host>.cms]".
   e. Escolha *Selecionar* e digite novamente todas as informações do banco de dados MySQL fornecidas durante a instalação (consulte as instruções de instalação).
   f. Quando tiver concluído, saia de cmsdbsetup.sh.
   g. ./stopservers
   h. ./startservers

   - Reinicialize o banco de dados MySQL:

   a. Efetue login como o usuário crystal.
   b. cd /opt/crystal_xi/bobje
   c. ./cmsdbsetup.sh
   d. Pressione Enter quando for exibido "[<nome_do_host>.cms]".
   e. Escolha *Reiniciar* e siga as instruções.
   f. Quando tiver concluído, saia de cmsdbsetup.sh.
   g. ./stopservers
   h. ./startservers

2. Verifique se todos os servidores CCM estão habilitados:

   a. Efetue login como o usuário crystal.
   b. cd /opt/crystal_xi/bobje
   c. ./ccm.sh -enable all

11 Configuração do Advisor

NOTA: O termo Agente é sinônimo de Coletor. De agora em diante, Agentes serão referidos como Coletores.

O Sentinel Advisor, ativado pela SecurityNexus, oferece inteligência em tempo real em relação a vulnerabilidades da empresa, orientação de especialistas e etapas recomendadas para a correção. Além disso, fornece uma referência cruzada entre assinaturas de ataque IDS em tempo real e sua base de conhecimento de vulnerabilidades. Visite o site http://www.esecurity.net/Software/Products/Advisor.asp para obter mais informações.

A instalação do Advisor é opcional. Porém, ele será um componente necessário se você quiser usar os recursos Sentinel Exploit Detection ou Advisor Reporting.

O Crystal BusinessObjects Enterprise™ 11 é uma das ferramentas de geração de relatórios que se integram ao Sentinel. Para obter informações sobre a instalação do Crystal BusinessObjects Enterprise™ 11, consulte o capítulo sobre *Crystal Reports* referente à plataforma na qual você deseja executar o Crystal Enterprise Server (Windows ou Linux). Caso use o Advisor somente para a Detecção de Exploração, não é necessário instalar o Crystal Server. Ele só é obrigatório se a intenção for executar relatórios.

Este capítulo discute como configurar o Sentinel para executar relatórios do Advisor diretamente do Sentinel Control Center. Os relatórios do Advisor são criados pela Novell para serem usados na geração e análise de relatórios e, depois que a integração do Sentinel Control Center é configurada corretamente, eles aparecem na guia Consultor do Sentinel Control Center.

Instalação do Advisor

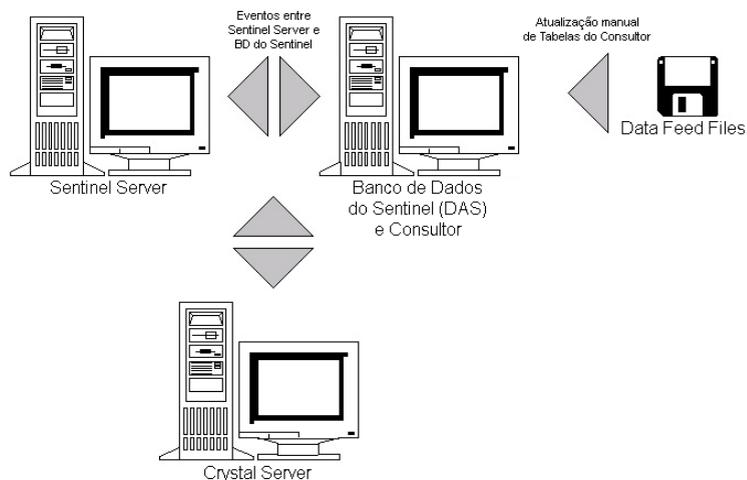
O Advisor só pode ser instalado na mesma máquina em que reside o DAS (Database Access Service).

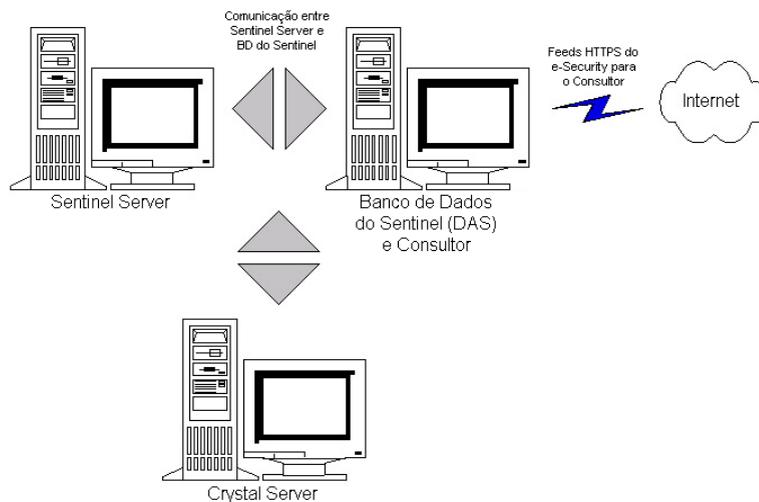
Há duas opções de instalação diferentes disponíveis. São elas:

- Independente
- Download Direto da Internet

Para executar o Crystal Reports do Advisor, primeiro consulte, no capítulo sobre *Crystal Reports*, a seção sobre instalação e configuração do Crystal Server. Em seguida, publique o Crystal Reports do Advisor no Crystal Server. Consulte Importando gabaritos de relatório para obter instruções sobre como publicar relatórios.

Configuração Independente

Na instalação Independente, o Advisor é um sistema isolado que requer intervenção manual para receber uma atualização da Novell.

Configuração Download Direto da Internet

Na instalação Download Direto da Internet, a máquina do Advisor está diretamente conectada à Internet. Nessa configuração, é feito o download automático das atualizações da Novell da Internet com regularidade.

Instalação do Advisor

NOTA: Antes de instalar o Advisor, verifique se tem o nome do usuário e a senha do Advisor fornecidos pela Novell. Durante a instalação, você será solicitado a fornecer o nome do usuário e a senha.

Se planejar executar relatórios do Advisor (Crystal Reports), execute o procedimento a seguir na ordem apresentada. Não é necessário realizar este procedimento se apenas quiser usar o Advisor para Detecção de Exploração.

- Se ainda não tiver feito isso, execute as seguintes ações (consulte o capítulo sobre *Crystal Reports*):
  - Instale o Microsoft Internet Information Server (IIS)
  - **Para o banco de dados do Sentinel no Oracle (Linux)** – pré-instalação do Crystal BusinessObjects Enterprise
  - Instale o Crystal BusinessObjects Enterprise™ 11
  - **Para o banco de dados do Sentinel no Oracle (Solaris)** – Configurar driver nativo do Oracle (para instalações do Oracle)
  - **Para o banco de dados do Sentinel no MS SQL (Windows)** – Configurar o Open Database Connectivity (ODBC)
  - Aplique o patch do Crystal Reports – consulte o capítulo sobre *Crystal Reports*.
- Instale o Advisor – se ele ainda não estiver instalado, consulte o capítulo *Adicionando componentes a uma instalação existente*.
- Importe gabaritos do Crystal Reports
- Cria uma página da Web Crystal
- Configure o Sentinel Control Center para integração com o Crystal Enterprise Server

Importando gabaritos de relatório

Dependendo do sistema operacional, consulte:

- *Capítulo 9 – Crystal Reports para Windows e Solaris*
- *Capítulo 10 – Crystal Reports para Linux*

Configurando o Administration Launchpad

Dependendo do sistema operacional, consulte:

- *Capítulo 9 – Crystal Reports para Windows e Solaris*
- *Capítulo 10 – Crystal Reports para Linux*

Configurando a integração do Sentinel Control Center com os relatórios do Advisor

Usando a guia Consultor, é possível integrar o Sentinel Control Center com os relatórios do Advisor. Usando esse recurso, você poderá ver um relatório do Advisor diretamente no Sentinel Control Center.

Para habilitar esse recurso, primeiro você deve instalar o Crystal Server, importar os gabaritos de relatório do Advisor no Crystal Server e, por último, instalar o Advisor. Depois de atendidas essas pré-condições, siga as instruções na seção “Configurando o Sentinel para integração com o Crystal Enterprise Server” no:

- *Capítulo 9 – Crystal Reports para Windows e Solaris*
- *Capítulo 10 – Crystal Reports para Linux*

Atualizando dados nas tabelas do Advisor

Se você não tiver uma configuração autônoma, os dados das tabelas do Advisor serão atualizados automaticamente durante o próximo download de alimentação do Consultor programado. No entanto, os dados também podem ser atualizados manualmente. Para atualizá-los manualmente, consulte o *Guia do Usuário do Sentinel*.

Redefinindo a senha do Advisor (somente Download Direto)

Se você estiver executando o Advisor no modo Download Direto e tiver obtido uma nova senha do Advisor ou se a senha definida durante a instalação estiver incorreta, será necessário redefinir a senha criptografada armazenada no arquivo de configuração do Advisor.

A atualização da senha criptografada do Advisor não se aplicará se você estiver executando o Advisor em uma configuração Independente porque, nesse modo, não é armazenada uma senha no arquivo de configuração do Advisor.

Para redefinir a senha criptografada armazenada no arquivo de configuração do Advisor, execute estas etapas:

1. No UNIX, efetue login como esecadm ou, no Windows, efetue login com direitos administrativos. Efetue login na máquina em que está instalado o Consultor.
2. Mude de diretório:

   Para o UNIX:

   ```
   $ESEC_HOME/sentinel/bin
   ```

   Para o Windows:

   ```
   %ESEC_HOME%\sentinel\bin
   ```

3. Execute este comando, em que <nova_senha> é a senha do Advisor que você deseja definir:

   Para o UNIX:

   ```
   ./adv_change_passwd.sh <nova_senha>
   ```

   Para o Windows:

   ```
   adv_change_passwd.bat <nova_senha>
   ```

12 Testando a instalação

NOTA: O termo Agente é sinônimo de Coletor. De agora em diante, Agentes serão referidos como Coletores.

Os Coletores de teste a seguir são instalados com o componente Serviço do Coletor (Gerenciador de Coletor) para ajudá-lo a testar a instalação. A seguir, é fornecida uma lista com o nome e a descrição de cada um desses coletores:

Para testar o fluxo de eventos básico:

- SendOneEvent – envia um evento pelo Sentinel e depois pára.
- SendMultipleEvents – envia 20 eventos pelo Sentinel e depois pára.

Para testar o mapeamento de bens de eventos e a detecção de ataques:

- DemoEvents – envia 13 eventos pelo Sentinel e depois pára.
- DemoAssetUpload – carrega dados de bens demo no Sentinel. Quando o coletor DemoEvents é executado após a execução deste coletor, os dados de bens deste coletor são exibidos nos eventos do coletor DemoEvents como resultado do mapeamento de eventos. Este coletor não gera eventos externos.
- DemoVulnerabilityUpload – carrega dados de vulnerabilidade demo no Sentinel. Quando o coletor DemoEvents é executado após a execução deste coletor e também após o download de alimentação do Consultor, alguns eventos do coletor DemoEvents acionam uma detecção de ataque (ou seja, o campo Vulnerabilidade do evento é definido como "1"). Este coletor não gera eventos externos.

Para obter mais informações (incluindo a configuração) sobre outros coletores, vá para:

```
%ESEC_HOME%\wizard\Elements\<Nome_do_coletor>\docs\
```

Testando a instalação com os coletores de teste

No Sentinel v5.1.2 e posterior, os coletores de teste são instalados previamente configurados em todos os Gerenciadores de Coletor. Portanto, se você estiver usando essa versão do Sentinel, poderá executar diretamente os coletores de teste para testar a sua instalação.

No Sentinel v5.1.1 e anteriores, você deve configurar manualmente os coletores em um Gerenciador de Coletor para poder usá-los. Para configurar os coletores de teste, siga as instruções na seção Configurando os coletores de teste. Em seguida, retorne a esta seção para testar a instalação usando os coletores de teste.

Executando os coletores de teste para testar a instalação

1. Abra o aplicativo Sentinel Control Center.
2. Clique na guia *Coletores*.
3. Na caixa de diálogo Gerenciador de Telas do Coletor, clique duas vezes em *TODOS OS AGENTES* para abrir uma tela em todas as portas do coletor.

4. A Tela do Coletor que aparece exibe todas as portas do coletor configuradas no momento, agrupadas pelo nome do Gerenciador de Coletor. Se não houver portas de coletor, isso significa que nenhum Gerenciador de Coletor está conectado ao Sentinel. Se você espera que um ou mais Gerenciadores de Coletor estejam conectados ao Sentinel, verifique se os Gerenciadores de Coletor estão em execução e se há erros nos arquivos de registro do Gerenciador de Coletor ou do Sentinel Server.
5. Antes de executar um coletor, abra uma Tela Ativa para ver os eventos gerados pelos coletores de teste. Para fazer isso:
   - Clique na guia *Telas Ativas*.
   - Selecione *Telas Ativas* > *Criar Tela Ativa* na barra de menus.
   - Selecione o filtro *PUBLIC::External_Events*.
   - Clique em *Concluir*.
6. Para executar um coletor a fim de testar o fluxo de eventos básico:
   - Vá para a guia *Coletores*.
   - Clique o botão direito do mouse na porta do coletor *SendMultipleEvents* na Tela do Coletor e selecione a ação Iniciar. Como os coletores de teste só são executados por um curto período de tempo e depois param, o status da porta do coletor mudará brevemente para "ativado" e, depois, de novo para "desativado".
   - Para verificar se os eventos estão fluindo pelo sistema, volte para a guia Telas Ativas e monitore a Tela Ativa criada. Observe que pode demorar um minuto para que o evento apareça na Tela Ativa depois de executar o coletor.
7. Para executar um coletor a fim de testar o mapeamento de bens de eventos:
   - Vá para a guia Coletores.
   - Clique o botão direito do mouse na porta do coletor *DemoAssetUpload* na Tela do Coletor e selecione a ação Iniciar. Como os coletores de teste só são executados por um curto período de tempo e depois param, o status da porta do coletor mudará brevemente para "ativado" e, depois, de novo para "desativado".
   - Aguarde alguns minutos para que os dados do bem sejam carregados no Sentinel, transformados em um mapa pelo Serviço de Mapeamento e distribuídos para os Gerenciadores de Coletor. Para saber quando isso acontece, procure um evento interno RefreshingMapFromServer com "Bem" na mensagem do evento. Para ver esse evento interno, você deve usar uma Tela Ativa com um filtro que permita a passagem de eventos internos (por exemplo, PUBLIC::Internal_Events). O filtro PUBLIC::External_Events não permite a passagem de eventos internos.
   - Clique o botão direito do mouse na porta do coletor *DemoEvents* na Tela do Coletor e selecione a ação Iniciar. Como os coletores de teste só são executados por um curto período de tempo e depois param, o status da porta do coletor mudará brevemente para "ativado" e, depois, de novo para "desativado".
   - Para verificar se ocorreram mapeamentos de bens de eventos, clique duas vezes em um evento (na tabela de eventos, na parte inferior da Tela Ativa) gerado pelo coletor DemoEvents para ver os detalhes do evento. Nos detalhes do evento exibidos à esquerda da tabela de eventos, expanda o grupo Bem para ver os dados do mapa de bens do evento. Observe que pode demorar um minuto para que o evento apareça na Tela Ativa depois de executar o coletor.

8. Para executar um coletor a fim de testar a detecção de exploração (exige a instalação do componente Advisor):

   - Execute o download de alimentação do Consultor (isso pode demorar um pouco):

   No Windows:

     - Faça login na máquina em que está instalado o Advisor. Execute a Tarefa Agendada do Advisor (*Iniciar* > *Painel de Controle* > *Tarefas Agendadas* > *{e-Security_Advisor | at1}*)

   No UNIX:

     - Efetue login na máquina em que o Advisor foi instalado como o usuário esecadm e execute:

   ```
   $ESEC_HOME/sentinel/bin/advisor.sh
   ```

   - No Sentinel Control Center, vá para a guia Coletores
   - Clique o botão direito do mouse na porta do coletor *DemoVulnerabilityUpload* na Tela do Coletor e selecione a ação Iniciar. Como os coletores de teste só são executados por um curto período de tempo e depois param, o status da porta do coletor mudará brevemente para "ativado" e, depois, de novo para "desativado".
   - Aguarde até que os dados atualizados de detecção de ataques sejam carregados no Gerenciador de Coletor. Para saber quando isso acontece, procure um evento interno RefreshingMapFromServer com "IsExploitWatchlist" na mensagem do evento. Para ver esse evento interno, você deve usar uma Tela Ativa com um filtro que permita a passagem de eventos internos (por exemplo, PUBLIC::Internal_Events). O filtro PUBLIC::External_Events não permite a passagem de eventos internos. Pode demorar um pouco mais de meia hora para que os dados atualizados de detecção de ataques sejam enviados ao Gerenciador de Coletor, pois, por padrão, o DAS atualiza os dados de detecção de ataques, no máximo, uma vez a cada 30 minutos.
   - Clique o botão direito do mouse na porta do coletor *DemoEvents* na Tela do Coletor e selecione a ação Iniciar. Como os coletores de teste só são executados por um curto período de tempo e depois param, o status da porta do coletor mudará brevemente para "ativado" e, depois, de novo para "desativado".
   - Para verificar se ocorreu detecção de ataques, clique duas vezes em um evento (na tabela de eventos, na parte inferior da Tela Ativa) gerado pelo coletor DemoEvents para ver os detalhes do evento. Nos detalhes do evento exibidos à esquerda da tabela de eventos, expanda o grupo Ataque para ver os dados da detecção de ataques. Em alguns eventos, o campo Vulnerabilidade pode ser definido como "1". Observe que pode demorar um minuto para que o evento apareça na Tela Ativa depois de executar o coletor.

Configurando os coletores de teste

No Sentinel v5.1.1 e anteriores, os coletores de teste não são previamente configurados durante a instalação. Portanto, você deve usar o Construtor de Coletor (em uma máquina Windows) para configurar os coletores antes de executá-los.

No Sentinel v5.1.2 e posterior, essas etapas de configuração não são necessárias, a menos que as portas de coletor de teste tenha sido apagadas.

Configurando o coletor SendOneEvent

Configurando, carregando e executando o coletor Enviar um Evento

1. Abra o aplicativo Construtor de Coletor.
2. Clique na guia *Hosts do Assistente*.
3. Realce o nome do host do computador. O nome do host aparece no campo abaixo do menu, na parte superior do aplicativo.
4. Clique duas vezes em *Novo…*, no cabeçalho Nome da Porta.
5. Digite um nome de porta de assistente (por exemplo, SendOneEvent).
6. Em Tipo de Rx/Tx, selecione *Nenhum*.
7. Deixe em branco o valor de Rx/Tx.
8. Na mesma linha, clique no menu suspenso da coluna Coletor e escolha SendOneEvent.
9. Clique em *Gravar*.
10. Clique na guia *Coletores*.
11. Expanda o coletor SendOneEvent.
12. Clique o botão direito do mouse no arquivo de gabarito *SendOneEvent* e, em seguida, em *Criar Scripts*.
13. Clique o botão direito do mouse no coletor *SendOneEvent* e, em seguida, em *Carregar Coletor*.
14. Na guia Coletores, selecione o computador. Clique em *Carregar*.
15. Se solicitado, digite a senha do Gerenciador de Coletor.
16. Clique em *OK*.

Configurando o coletor SendMultipleEvents

Configurando, carregando e executando o coletor Enviar Vários Eventos

1. Abra o aplicativo Construtor de Coletor.
2. Clique na guia *Hosts do Assistente*.
3. Realce o nome do host do computador. O nome do host aparece no campo abaixo do menu, na parte superior do aplicativo.
4. Clique duas vezes em Novo… sob o cabeçalho Nome da Porta, digite um nome de porta de assistente (por exemplo, SendMultipleEvents).
5. Na mesma linha, clique no menu suspenso da coluna Tipo de Rx/Tx e escolha Todos os Arquivos.
6. Na mesma linha, clique na caixa de texto da coluna Valor de Rx/Tx e digite o caminho do arquivo de entrada:

```
Elements\SendMultipleEvents\config\test_events.csv
```

7. Na mesma linha, clique no menu suspenso da coluna Coletor e escolha SendMultipleEvents.
8. Clique em *Gravar*.
9. Clique na guia *Coletores*.
10. Expanda o coletor SendMultipleEvents.

11. Clique o botão direito do mouse no arquivo de gabarito *SendMultipleEvents* e, em seguida, em *Criar Scripts*.
12. Clique o botão direito do mouse no coletor *SendMultipleEvents* e, em seguida, em *Carregar Coletor*.
13. Na guia Coletores, selecione o computador. Clique em *Carregar*.
14. Se solicitado, digite a senha do Gerenciador de Coletor.
15. Clique em *OK*.

Configurando o coletor DemoEvents

Configurando, carregando e executando o coletor DemoEvents

1. Abra o aplicativo Construtor de Coletor.
2. Clique na guia *Hosts de Assistentes*.
3. Realce o nome do host do computador. O nome do host aparece no campo abaixo do menu, na parte superior do aplicativo.
4. Clique duas vezes em Novo… sob o cabeçalho Nome da Porta, digite um nome de porta de assistente (por exemplo, DemoEvents).
5. Na mesma linha, clique no menu suspenso da coluna Tipo de Rx/Tx e escolha Todos os Arquivos.
6. Na mesma linha, clique na caixa de texto da coluna Valor de Rx/Tx e digite o caminho do arquivo de entrada:

   ```
   Elements\DemoEvents\data\Generic_Events.csv
   ```

7. Na mesma linha, clique no menu suspenso da coluna Coletor e escolha DemoEvents.
8. Clique em *Gravar*.
9. Clique em *Carregar*.
10. Selecione a guia *Coletores*.
11. Clique na seta para baixo e selecione o coletor DemoEvents.
12. Clique em *Carregar*.
13. Se solicitado, digite a senha do Gerenciador de Coletor.
14. Clique em *OK*.

Configurando o coletor DemoAssetUpload

Configurando, carregando e executando o coletor DemoAssetUpload

1. Abra o aplicativo Construtor de Coletor.
2. Clique na guia *Hosts de Assistentes*.
3. Realce o nome do host do computador. O nome do host aparece no campo abaixo do menu, na parte superior do aplicativo.
4. Clique duas vezes em *Novo*… no cabeçalho *Nome da Porta* e digite um nome de porta de assistente (por exemplo, DemoAssetUpload).
5. Na mesma linha, clique no menu suspenso da coluna Tipo de Rx/Tx e escolha Todos os Arquivos.

6. Na mesma linha, clique na caixa de texto da coluna Valor de Rx/Tx e digite o caminho do arquivo de entrada:

   ```
   Elements\DemoAssetUpload\data\asset_info.csv
   ```

7. Na mesma linha, clique no menu suspenso da coluna Coletor e escolha DemoAssetUpload.
8. Clique em *Gravar*.
9. Clique em *Carregar*.
10. Selecione a guia *Coletores*.
11. Clique na seta para baixo e selecione DemoAssetUpload.
12. Clique em *Carregar*.
13. Se solicitado, digite a senha do Gerenciador de Coletor.
14. Clique em *OK*.

Configurando o coletor DemoVulnerabilityUpload

Configurando, carregando e executando o coletor DemoVulnerabilityUpload

1. Abra o aplicativo Construtor de Coletor.
2. Clique na guia *Hosts de Assistentes*.
3. Realce o nome do host do computador. O nome do host aparece no campo abaixo do menu, na parte superior do aplicativo.
4. Clique duas vezes em *Novo*… no cabeçalho Nome da Porta e digite um nome de porta de assistente (por exemplo, DemoVulnerabilityUpload).
5. Na mesma linha, clique no menu suspenso da coluna Tipo de Rx/Tx e escolha Todos os Arquivos.
6. Na mesma linha, clique na caixa de texto da coluna Valor de Rx/Tx e digite o caminho do arquivo de entrada:

   ```
   Elements\DemoVulnerabilityUpload\data\vuln_info.csv
   ```

7. Na mesma linha, clique no menu suspenso da coluna Coletor e escolha DemoVulnerabilityUpload.
8. Clique em *Gravar*.
9. Clique em *Carregar*.
10. Selecione a guia *Coletores*.
11. Clique na seta para baixo e selecione o coletor DemoVulnerabilityUpload.
12. Clique em *Carregar*.
13. Digite a senha do Gerenciador de Coletor.
14. Clique em *OK*.

13 Fazendo mudanças na camada de comunicação (iSCALE)

NOTA: O termo Agente é sinônimo de Coletor. De agora em diante, Agentes serão referidos como Coletores.

iSCALEA camada de comunicação (iSCALE) que conecta todos os componentes da arquitetura consiste em uma conexão baseada em TCP/IP criptografada. Por padrão, essa comunicação é criptografada usando AES de 256 bits. O ARC4 está disponível para uso.

O keymgr permite escolher o método de criptografia a ser usado e também mudar a chave. O programa gera um arquivo no diretório lib de uma instalação do Sentinel ($ESEC_HOME/lib ou %ESEC_HOME%\lib) chamado .keystore. Esse arquivo deve ser copiado em cada máquina em que um componente do Sentinel tenha sido instalado.

O Sentinel recomenda como melhor prática que a chave de segurança padrão seja mudada para fornecer parâmetros exclusivos de criptografia e autenticação.

NOTA: Se você estiver usando o conector Consultor, DBConnector ou RDEP Collector, deverá atualizar as senhas armazenadas nos arquivos de configuração de cada um desses componentes. Isso é necessário porque a chave criptográfica usada para criptografar a senha antes de ser armazenada nesses arquivos de configuração se baseia na chave no arquivo .keystore que é atualizado.

Fazendo mudanças na chave criptográfica

Fazendo mudanças de chave ou habilitando outros métodos de criptografia

1. No UNIX, efetue login como esecadm. No Windows, efetue login como um usuário com direitos administrativos.
2. Use o comando cd para mudar o diretório:

   Para o Windows:

   ```
   %ESEC_HOME%\lib
   ```

   Para o UNIX:

   ```
   $ESEC_HOME/lib
   ```

3. Execute o seguinte comando:

   No Windows:

   ```
   "%ESEC_JAVA_HOME%\java" -jar keymgr.jar -–keyalgo
      <criptografia [AES ou ARC4]> --keysize 256
   ```

No UNIX:

```
$ESEC_JAVA_HOME/java -jar keymgr.jar -–keyalgo
   <criptografia [AES ou ARC4]> --keysize 256
```

Isso permite definir o método de criptografia. Será criado um arquivo chamado .keystore no diretório lib.

4. Copie .keystore em cada máquina com um componente do Sentinel instalado. O arquivo deve ser copiado em:

   Para o Windows:

   ```
   %ESEC_HOME%
   ```

   Para o UNIX:

   ```
   $ESEC_HOME
   ```

5. Se você tiver o conector DBConnector ou RDEP Collector configurado em qualquer máquina do Gerenciador de Coletor, deverá atualizar as senhas em todas as instâncias do arquivo de configuração do conector. Isso é necessário porque a chave criptográfica usada para criptografar a senha antes de ser armazenada no arquivo de configuração do conector se baseia na chave no arquivo .keystore que acabou de ser atualizado. Para obter instruções sobre a definição de senhas nos arquivos de configuração do conector, consulte a documentação dos conectores DBConnector e RDEP Collector.
6. Se você estiver executando o Consultor no modo Download Direto no sistema, será necessário atualizar a senha criptografada do Consultor armazenada em seu arquivo de configuração. Isso é necessário porque a chave criptográfica usada para criptografar a senha antes de ser armazenada no arquivo de configuração do Consultor se baseia na chave no arquivo .keystore recém-atualizado. A atualização da senha criptografada do Consultor não será aplicável se você estiver executando o Consultor em uma configuração independente, porque, nesse modo, nenhuma senha é armazenada no arquivo de configuração do Consultor. Para atualizar a senha criptografada armazenada no arquivo de configuração do Consultor, execute estas etapas na ordem apresentada:
   - No UNIX, faça login como esecadm ou, no Windows, faça login com direitos administrativos. Efetue login na máquina em que está instalado o Consultor.
   - Mude de diretório:

   Para o UNIX:

   ```
   $ESEC_HOME/sentinel/bin
   ```

   Para o Windows:

   ```
   %ESEC_HOME%\sentinel\bin
   ```

   - Digite os seguintes comandos:

   Para o UNIX:

   ```
   ./adv_change_passwd.sh <nova_senha>
   ```

   Para o Windows:

   ```
   adv_change_passwd.bat <nova_senha>
   ```

14 Adicionando componentes a uma instalação existente

NOTA: O termo Agente é sinônimo de Coletor. De agora em diante, Agentes serão referidos como Coletores.

O instalador do Sentinel 5 Enterprise Security Management permite adicionar componentes do Sentinel a uma instalação existente. Um exemplo da adição de um componente seria instalar apenas o Gerenciador de Coletor do Assistente em uma máquina e, posteriormente, decidir que o Sentinel Control Center também deve ser instalado nessa máquina. Nesse caso, você adicionaria o componente Sentinel Control Center à instalação do Gerenciador de Coletor do Assistente.

NOTA: Antes de adicionar um componente, verifique se as variáveis corretas do Sentinel foram definidas.

```
ESEC_HOME
ESEC_JAVA_HOME
WORKBENCH_HOME
ESEC_CONF_FILE
ESEC_VERSION
ESEC_USER
LD_LIBRARY_PATH
```

Adicionando componentes no Solaris ou Linux

Adicionando componentes no Solaris

1. Faça login como Usuário Root.
2. Insira e monte o CD de instalação do Sentinel.
3. Para iniciar o programa de instalação, vá para o diretório de instalação no CD-ROM e digite:

   ```
   ./setup.sh
   ```

   ou

   ```
   ./setup.sh –console (se o X Windows não estiver
     disponível)
   ```

4. Será exibida uma mensagem indicando o local da instalação anterior e os componentes que já estão instalados. Clique em *Avançar*.
5. Escolha os componentes que deseja adicionar e clique em *Avançar*.
6. Siga os prompts, digitando as informações apropriadas. Para obter mais informações sobre um determinado prompt, consulte o capítulo de instalação correspondente.

Adicionando componentes no Windows

Adicionando componentes no Windows

1. Insira o CD de instalação do Sentinel na unidade de CD-ROM.
2. Procure o CD e clique duas vezes em setup.bat.

NOTA: Não há suporte para a instalação no modo de console no Windows.

3. Na tela de boas-vindas, clique em *Avançar*.
4. Aceite o Contrato de Licença de Usuário Final e clique em *Avançar*.
5. Será exibida uma mensagem indicando o local da instalação anterior e os componentes que já estão instalados. Clique em *Avançar*.
6. Escolha os componentes que deseja adicionar e clique em *Avançar*.
7. Siga os prompts, digitando as informações apropriadas. Para obter mais informações sobre um determinado prompt, consulte o *capítulo 3* (para Solaris), o *capítulo 4* (para Linux) ou o *capítulo 5* (para Windows).

15 Desinstalando o software

NOTA: O termo Agente é sinônimo de Coletor. De agora em diante, Agentes serão referidos como Coletores.

Desinstalando o Sentinel, o Gerenciador de Coletor e o Consultor

Desinstalação no Solaris e Linux

Iniciando o desinstalador do Sentinel para Solaris

1. Faça login como Usuário Root.
2. Pare o Sentinel Server.
3. Use o comando cd para mudar o diretório:

```
$ESEC_HOME/_uninst
```

4. Digite:

```
./uninstall.bin
```

NOTA: No Solaris e no Linux, após a desinstalação do Sentinel Server, você precisará remover manualmente o usuário esecadm do sistema operacional, se desejar.

Desinstalação no Windows

Usando o Desinstalador do Sentinel para Windows

5. Efetue login como Administrador.
6. Pare o Sentinel Server.
7. Selecione Iniciar > Arquivos de Programas > Sentinel > Desinstalar o Sentinel 5.x.
8. Siga os prompts na tela. Selecione os aplicativos a desinstalar:
   - Banco de Dados
   - Servidor de Comunicação (barramento de mensagens)
   - Consultor
   - Serviços do Sentinel de Base
   - Correlação
   - DAS
   - Serviço do Coletor (Gerenciador de Coletor)
   - Sentinel Control Center

- Sentinel Database Manager (SDM)
- HP OpenView Service Desk
- Integração do Remedy

Desinstalando com o Painel de Controle

Para desinstalar os aplicativos Windows do Sentinel

9. Clique em Iniciar > Programas > Configurações > Painel de Controle > Adicionar ou Remover Programas.
10. Clique em Sentinel 5.x.
11. Siga os prompts. Você será solicitado a selecionar o aplicativo a ser desinstalado. Selecione os aplicativos que deseja desinstalar.

Pós-desinstalação

A desinstalação deixa alguns arquivos na máquina, assim, você precisará apagá-los manualmente após desinstalar o Sentinel 5. Talvez seja necessário apagar o diretório $ESEC_HOME ou %ESEC_HOME% e todos os subdiretórios. No caso do Consultor, você pode apagar as pastas de ataque e alerta usadas para arquivos de dados do Consultor.

Alguns arquivos que permanecem são:

- Arquivos de registro do Sentinel
- Arquivos de registro do Assistente
- Arquivos de registro do DAS
- Arquivos de registro do Gerenciador de Coletor

Ocasionalmente, após uma desinstalação, ainda restam configurações do sistema. Consulte o *Apêndice E* para obter procedimentos para remover manualmente as configurações do sistema restantes.

Questionário de pré-instalação

NOTA: Para usuários do MS SQL 2000, o tamanho do evento não pode ser maior que 8KB.

NOTA: O termo Agente é sinônimo de Coletor. De agora em diante, Agentes serão referidos como Coletores.

Questões pré-instalação

1. Após determinar qual máquina será sua máquina DAS e que ela corresponde a todos os requisitos de OS e hardware necessários:
   a. Obtenha o número de ID de host da máquina DAS
   b. Contate a Novell e obtenha a chave de licença
2. Qual o seu objetivo ou propósito ao usar o Novell Sentinel?
   a. Conformidade
   b. SEM
   c. Outros____
3. Qual é a arquitetura de rede para os dispositivos de origem com relação ao segmento de segurança no qual o hardware do Sentinel/Assistente será localizado?

   NOTA: Isto é importante para compreender a hierarquia do assistente de coleta de dados e para identificar todos os firewalls que devem ser penetrados para ativar a comunicação do Assistente para o Sentinel ou a comunicação do Sentinel para o BD ou ainda a comunicação do Crystal Server para o BD.

   Digite as informações abaixo (texto e/ou desenho) ou link para a informação.

4. Que relatórios você quer retirar do sistema? Isto é importante para garantir que os coletores reúnam os dados corretos para serem passados para o banco de dados do Sentinel.
   a. ____
   b. ____
   c. ____
   d. ____
   e. ____
   f. ____
5. De quais dispositivos de origem você deseja coletar dados (IDS, HIDS, Roteadores, Firewalls, etc...), taxas de eventos (EPS - eventos por segundo), versões, métodos de conexão, plataformas e patches?

Dispositivo (mfr/modelo)	**Taxa de eventos (EPS)**	**Versão**	**Método de conexão**	**Plataforma**	**Patches**

   Você pode oferecer exemplos dos dados que você deseja que os coletores do Sentinel coletem e analisem? Isso é importante para que o Sentinel possa oferecer o que você precisa.
6. Quais padrões/modelos de segurança existem no seu site?
   - Qual a sua postura em relação a contas locais versus autenticação de domínio?
     - Para Windows com autenticação de domínio, configurações de conta de domínio apropriado devem ser criadas para garantir que o Sentinel possa ser instalado.
     - Para as instalações do Solaris isso não se aplica. Contudo, o Sentinel não tem suporte para NIS.
7. Qual hardware foi alocado para a instalação do Sentinel? Ele está de acordo com as especificações de hardware fornecidas nos Capítulos 1 e 2 do Guia de Instalação?
8. Qual a retenção de dados necessária por dia? Geralmente 30 dias é bom. O MS SQL apresenta dificuldades com mais de 60 dias. O Oracle é OK.

9. Com base nas informações de retenção de dados e EPS, qual tamanho de disco será usado? Use 500 a 800 bytes/evento para estimativas de tamanho.
10. Você validou os requisitos do Sentinel para operar contra a sua configuração como nos Capítulos 1 e 2 do Guia de Instalação?
    - Níveis de patch do OS
    - Patches de serviços
    - Hot Fixes, etc.

Manutenção pré e pós instalação para Banco de Dados Oracle em Solaris

NOTA: O termo Agente é sinônimo de Coletor. De agora em diante, Agentes serão referidos como Coletores.

Lista de verificação pré-instalação

Essa lista de verificação pré-instalação do Oracle é destinada inicialmente a instalações distribuídas. Porém, ela também pode ser usada para instalações individuais. Se o número de instâncias do Gerenciador de Coletores e do Mecanismo de Correlação for maior que três, anote-os. Essa lista de verificação permite instâncias do Gerenciador de Coletores e do Mecanismo de Correlação igual ou menor a três.

Para obter mais informações, consulte o Capítulo 3 - Instalando o Sentinel 5 para Oracle.

	Variável de configuração			
1.	*Versão do Sentinel:*			*Data de hoje:*
	Sistema operacional			
	▪ OS correto para DB	: Sim | : Não	▪ Patch adequado	: Sim | : Não
	▪ Oracle DB w correto/ Particionamento	: Sim | : Não	▪ Patch adequado	: Sim | : Não
	▫ Versão		▫ Nível de patch	
	▪ Cópia do Oracle Note: 148673.1	: Sim | : Não		
	▪ Conjunto de variáveis de ambiente para o usuário do sistema operacional Oracle.	: Sim | : Não		
	▪ Sistema operacional correto para Componentes do Sentinel	: Sim | : Não	▪ Patch adequado	: Sim | : Não
2.	*Máquina DAS*			
	▪ ID de host			
	▪ número de série			
	▪ chave de licença			
3.	*Install DAS (Instalar DAS)*			
	▪ Nome de host ou IP do Banco de Dados			Padrão: ESEC
	▪ Nome do banco de dados			Padrão: 1521
	▪ Porta do banco de dados			
	▪ Local do arquivo JDBC			

	Variável de configuração			
4.	*Valores de Kernel UNIX para o Oracle. Abaixo, os valores mínimos.*			
	▪ shminfo_shmmax	4294967295	: Sim | : Não	Valor se maior:
	▪ shminfo_shmmin	1	: Sim | : Não	Valor se maior:
	▪ shminfo_shmseg	50	: Sim | : Não	Valor se maior:
	▪ shminfo_shmmni	400	: Sim | : Não	Valor se maior:
	▪ seminfo_semmns	14000	: Sim | : Não	Valor se maior:
	▪ seminfo_semmni	1024	: Sim | : Não	Valor se maior:
	▪ seminfo_semmsl	1024	: Sim | : Não	Valor se maior:
	▪ seminfo_shmopm	100	: Sim | : Não	Valor se maior:
	▪ seminfo_shmvmx	32767	: Sim | : Não	Valor se maior:
5.	*Instância do Banco de Dados (SID)*			
6.	*Nome do banco de dados*			
7.	*Componentes do Sentinel:*			
	▪ Banco de Dados do Sentinel (IP ou DNS)			OS: Patch:
	▫ Registro de instalação do banco de dados			
	▫ Memória Oracle (RAM)			
	▫ Nome da instância			
	▫ Porta de escuta		Padrão: 1521	
	▫ Senha do SISTEMA			
	▫ Senha do SISTEMA			
	▪ Servidor de Comunicação (iSCALE) (IP ou DNS)			OS: Patch:
	▪ Serviços de Base do Sentinel (IP ou DNS)			OS: Patch:
	▪ DAS/Consultor (IP ou DNS) (O consultor é opcional)			OS: Patch:
	▫ DAS RAM			
	▪ Mecanismo de Correlação (IP e OS)			
		IP:		OS:

	Variável de configuração		
		IP:	OS:
		IP:	OS:
	▪ Crystal Server (IP ou DNS)		
	▫ MS SQL (Opcional, mas recomendado)	Versão do MS SQL: Patch do MS SQL: sa password or holder of password:	
	▪ Construtor de Coletores (IP ou DNS) (recomenda-se uma instalação)		
	▪ Gerenciador de Coletores (Serviços de Coletor)	**NOTA**: O Gerenciador de Coletores pode ser definido sem uma senha.	
	▫ IP: ▫ IP: ▫ IP:	PW: PW: PW:	OS: OS: OS:
8.	*Consultor (opcional)*		
	▪ Local do arquivo de alimentação de dados		
	▪ Consultor endereço para		
	▪ Consultor endereço para		
	▪ Nome de usuário e senha	u/n:	PW:
9.	*Locais de arquivo do banco de dados:*		
	▪ Arquivos de dados		
	▪ Arquivos de índice		
	▪ Arquivos de dados de resumo		
	▪ Arquivos de índice de resumo		
	▪ Arquivos Temporário e Desfazer Tabela		
	▪ Diretório A do Membro de Redo Log		
	▪ Diretório A do Membro de Redo Log		
10.	*Tamanho do banco de dados:*		
	▪ Padrão (20 GB)		
	▪ Grande (400 GB)		
	▪ Personalizado (tamanho)		
11.	*SMTP Server (DNS ou IP)*		

	Variável de configuração		
12.	*Senhas de usuário*		
	▪ esecadm	PW:	Padrão: /export/home
	▫ Diretório pessoal		
	▪ esecapp	PW:	
	▪ esecdba	PW:	
	▪ esecrpt	PW:	

Manutenção pós-instalação

Há alguns utilitários disponíveis para periodicamente realizar a manutenção do banco de dados. Esses utilitários incluem:

- Analisar partições – reúne estatísticas de partições que foram recentemente preenchidas.
- Analisar tabelas – reúne estatísticas globais de tabelas para os eventos e as tabelas de eventos correlacionadas.
- Verificação da saúde do banco de dados – reúne informações sobre o banco de dados. Ele relata:
  - se a instância do Banco de Dados está alta
  - se a escuta do Oracle está alta
  - o uso do espaço
  - índices não utilizáveis
  - objetos inválidos do banco de dados
  - análises do banco de dados

Para obter mais informações, consulte o *Capítulo 2 - Melhores práticas, seção Melhores práticas de manutenção.*

Um aplicativo chamado Gerenciador de Dados do Sentinel é fornecido com o Sentinel. Use esse aplicativo para gerenciar o banco de dados. Para obter mais informações, consulte o *Guia do Usuário do Sentinel, Capítulo 10 – Gerenciador de Dados do Sentinel*.

C Manutenção pré e pós instalação para Banco de Dados Oracle no Linux

NOTA: O termo Agente é sinônimo de Coletor. De agora em diante, Agentes serão referidos como Coletores.

Lista de verificação pré-instalação

Essa lista de verificação pré-instalação do Oracle é destinada inicialmente a instalações distribuídas. Porém, ela também pode ser usada para instalações individuais. Se o número de instâncias do Gerenciador de Coletores e do Mecanismo de Correlação for maior que três, anote-os. Essa lista de verificação permite instâncias do Gerenciador de Coletores e do Mecanismo de Correlação igual ou menor a três.

Para obter mais informações, consulte o *Capítulo 3 - Instalando o Sentinel 5 para Oracle*.

	Variável de configuração			
1.	*Versão do Sentinel:*			*Data de hoje:*
	Sistema operacional			
	▪ OS correto para DB	: Sim | : Não	▪ Patch adequado	: Sim | : Não
	▫ Versão		▫ Nível de patch	
	▪ BD Oracle correto c/ Particionamento	: Sim | : Não	▪ Patch adequado	: Sim | : Não
	▫ Versão		▫ Nível de patch	
	▪ Variáveis de ambiente corretas definidas para o usuário do sistema operacional Oracle.	: Sim | : Não		
	▪ Script de inicialização (máquina DB)	: Sim | : Não		
	▪ Processos (máquina DB)	: Sim | : Não		
	▪ Soquetes	: Sim | : Não		
	▪ Sistema operacional correto para Componentes do Sentinel	: Sim | : Não	▪ Patch adequado	: Sim | : Não
2.	*Máquina DAS*			
	▪ ID de host			
	▪ número de série			
	▪ chave de licença			
3.	*Install DAS (Instalar DAS)*			
	▪ Nome de host ou IP do Banco de Dados			
	▪ Nome do banco de dados			Padrão: ESEC

	Variável de configuração		
	▪ Porta do banco de dados		Padrão: 1521
	▪ Local do arquivo JDBC		
4.	*Valores de Kernel UNIX para o Oracle. Abaixo, os valores mínimos.*		
	▪ shmmax	2147483648 : Sim | : Não	Valor se maior:
	▪ shmmin	1 : Sim | : Não	Valor se maior:
	▪ shmseg	4096 : Sim | : Não	Valor se maior:
	▪ shmmni	400 : Sim | : Não	Valor se maior:
	▪ semmns	500 : Sim | : Não	Valor se maior:
	▪ semmni	1024 : Sim | : Não	Valor se maior:
	▪ semmsl	1024 : Sim | : Não	Valor se maior:
	▪ shmopm	100 : Sim | : Não	Valor se maior:
	▪ shmvmx	32767 : Sim | : Não	Valor se maior:
5.	*Instância do Banco de Dados (SID)*		
6.	*Nome do banco de dados*		
7.	*Componentes do Sentinel:*		
	▪ Banco de Dados do Sentinel (IP ou DNS)		OS: Patch:
	▫ Registro de instalação do banco de dados		
	▫ Memória Oracle (RAM)		
	▫ Nome da instância		
	▫ Porta de escuta	Padrão: 1521	
	▫ Senha do SISTEMA		
	▫ Senha do SISTEMA		
	▪ Servidor de Comunicação (iSCALE) (IP ou DNS)		OS: Patch:
	▪ Serviços de Base do Sentinel (IP ou DNS)		OS: Patch:
	▪ DAS/Consultor (IP ou DNS) (O consultor é opcional)		OS: Patch:
	▫ DAS RAM		
	▪ Mecanismo de Correlação (IP e OS)		

	Variável de configuração			
		▫ IP:		OS:
		▫ IP:		OS:
		▫ IP:		OS:
	▪ Crystal Server (IP ou DNS)			
	▫ MS SQL (Opcional, mas recomendado)	Versão do MS SQL: Patch do MS SQL: senha sa ou portador de senha		
	▪ Construtor de Coletores (IP ou DNS) (recomenda-se uma instalação)			
	▪ Gerenciador de Coletores (Serviços de Coletor)	**NOTA**: O Gerenciador de Coletores pode ser definido sem uma senha.		
	▫ IP:	u/n:	PW:	OS:
	▫ IP:	u/n:	PW:	OS:
	▫ IP:	u/n:	PW:	OS:
8.	*Consultor (opcional)*			
	▪ Local do arquivo de alimentação de dados			
	▪ Endereço de origem do Consultor			
	▪ Endereço de destino do Consultor			
	▪ Nome de usuário e senha	u/n:		PW:
9.	*Locais de arquivo do banco de dados:*			
	▪ Arquivos de dados			
	▪ Arquivos de índice			
	▪ Arquivos de dados de resumo			
	▪ Arquivos de índice de resumo			
	▪ Arquivos Temporário e Desfazer Tabela			
	▪ Diretório A do Membro de Redo Log			
	▪ Diretório A do Membro de Redo Log			
10.	*Tamanho do banco de dados:*			
	▪ Padrão (20 GB)			
	▪ Grande (400 GB)			
	▪ Personalizado (tamanho)			
11.	*SMTP Server (DNS ou IP)*			

	Variável de configuração		
12.	*Senhas de usuário*		
	▪ esecadm	PW:	
	▫ Diretório pessoal		Padrão: /export/home
	▪ esecapp	PW:	
	▪ esecdba	PW:	
	▪ esecrpt	PW:	

Manutenção pós-instalação

Há alguns utilitários disponíveis para periodicamente realizar a manutenção do banco de dados. Esses utilitários incluem:

- Analisar partições – reúne estatísticas de partições que foram recentemente preenchidas.
- Analisar tabelas – reúne estatísticas globais de tabelas para os eventos e as tabelas de eventos correlacionadas.
- Verificação da saúde do banco de dados – reúne informações sobre o banco de dados. Ele relata:
  - se a instância do Banco de Dados está alta
  - se a escuta do Oracle está alta
  - o uso do espaço
  - índices não utilizáveis
  - objetos inválidos do banco de dados
  - análises do banco de dados

Para obter mais informações, consulte o *Capítulo 2 - Melhores práticas, seção Melhores práticas de manutenção*.

Um aplicativo chamado Gerenciador de Dados do Sentinel é fornecido com o Sentinel. Use esse aplicativo para gerenciar o banco de dados. Para obter mais informações, consulte o *Guia do Usuário do Sentinel, Capítulo 10 – Gerenciador de Dados do Sentinel*.

Manutenção pré e pós instalação para Banco de Dados MS SQL no Windows

NOTA: O termo Agente é sinônimo de Coletor. De agora em diante, Agentes serão referidos como Coletores.

NOTA: Para usuários do MS SQL 2000, o tamanho do evento não pode ser maior que 8KB.

Lista de verificação pré-instalação

Essa lista de verificação pré-instalação do MS SQL é destinada inicialmente a instalações distribuídas. Porém, ela também pode ser usada para instalações individuais. Se o número de instâncias do Gerenciador de Coletores e do Mecanismo de Correlação for maior que três, anote-os. Essa lista de verificação permite instâncias do Gerenciador de Coletores e do Mecanismo de Correlação igual ou menor a três.

Para obter mais informações, consulte o *Capítulo 4 - Instalando o Sentinel 5 para MS SQL*.

	Variável de configuração			
1.	*Versão do Sentinel:*			*Data de hoje:*
	Sistema operacional			
	▪ SO correto para DB	: Sim | : Não	▪ Patch adequado	: Sim | : Não
	▪ BD SQL correto	: Sim | : Não	▪ Patch adequado	: Sim | : Não
	▫ Versão		▫ Nível de patch	
	▪ Sistema operacional correto para Componentes do Sentinel	: Sim | : Não	▪ Patch adequado	: Sim | : Não
2.	*Para instalação DAS em Conta de Domínio Windows, atribua 'Fazer login como serviço'*	: Sim | : Não		
3.	*Máquina DAS*			
	▪ ID de host			
	▪ número de série			
	▪ chave de licença			
4.	*Nome de host do banco de dados ou IP:*	*<nome de host>[\<nome de instância>]*		
5.	*Nome do banco de dados:*			Padrão: ESEC
6.	*Porta:*		Padrão: 1433	

	Variável de configuração		
7.	*Install SQL (Instalar SQL)*	: mista : não mista	
8.	*Senha sa de servidor SQL ou portador de senha.*	PW:	
9.	*Componentes do Sentinel:*		
	▪ Banco de Dados do Sentinel (IP ou DNS)		OS: Patch:
	▪ Servidor de Comunicação (iSCALE) (IP ou DNS)		OS: Patch:
	▪ Serviços de Base do Sentinel (IP ou DNS)		OS: Patch:
	▪ DAS/Consultor (IP ou DNS) (O consultor é opcional)		OS: Patch:
	▪ Mecanismo de Correlação (IP e OS)		
		IP:	OS:
		IP:	OS:
		IP:	OS:
	▪ Crystal Server (IP ou DNS)		OS: Patch:
	▫ MS SQL (Opcional, mas recomendado)	Versão do MS SQL: Patch do MS SQL: senha sa ou portador de senha:	
	▪ Construtor de Coletores (IP ou DNS) (recomenda-se uma instalação)		
	▪ Gerenciador de Coletores (senhas de Serviços de Coletor w/ IP ou DNS e OS)	**NOTA**: O Gerenciador de Coletores pode ser definido sem uma senha.	
	▫ IP: ▫ IP: ▫ IP:	PW: PW: PW:	OS: OS: OS:
10.	*Consultor (opcional)*		
	▪ Local do arquivo de alimentação de dados		
	▪ Endereço de do Consultor		
	▪ Endereço para do Consultor		
	▪ Nome de usuário e senha	u/n:	PW:

	Variável de configuração		
11.	*Locais de arquivo do banco de dados:*		
	▪ Arquivos de dados		
	▪ Arquivos de índice		
	▪ Arquivos de dados de resumo		
	▪ Arquivos de índice de resumo		
	▪ Arquivos de registro		
12.	*Tamanho do banco de dados:*		
	▪ Padrão (20 GB)		
	▪ Grande (400 GB)		
	▪ Personalizado (tamanho)		
13.	*SMTP Server (DNS ou IP)*		
14.	*Para autenticação SQL (senhas)*		
	▪ esecadm	PW:	
	▪ esecapp	PW:	
	▪ esecdba	PW:	
	▪ esecrpt	PW:	
15.	*Para autenticação do Windows (senhas)*		
	▪ DBA (login)	u/n:	
	▪ Usuário do aplicativo (login e senha)	u/n:	PW:
	▪ Administrador do Sentinel (login)	u/n:	
	▪ Usuário de Geração de Relatórios do Sentinel (login)	u/n:	

Manutenção pós-instalação

O sistema operacional do Windows permite arquivar dados e adicionar partições automaticamente. Para obter mais informações, consulte o Capítulo 2 - Melhores práticas, seção Arquivando dados e adicionando partições automaticamente.

Limpeza manual de instalações anteriores

NOTA: O termo Agente é sinônimo de Coletor. De agora em diante, Agentes serão referidos como Coletores.

Ao realizar uma instalação limpa do Sentinel é altamente recomendado executar todas as etapas a seguir para ter certeza de que arquivos e configurações do sistema que podem ter sobrado de uma instalação anterior do Sentinel impeçam a nova instalação limpa. Execute as etapas seguintes em cada máquina onde esteja sendo feita uma instalação limpa antes de executar o instalador.

CUIDADO: Essas instruções envolvem a modificação de configurações e arquivos do sistema operacional. Se você não estiver familiarizado com a modificação dessas configurações e/ou arquivos do sistema, contate o Administrador do Sistema.

Solaris

Limpeza manual do Sentinel no Solaris

1. Efetue login como Usuário Root.
2. Verifique se todos os processos do Sentinel não estão sendo executados.
3. Remova os conteúdos de /opt/sentinelXX (ou onde o software do Sentinel tenha sido instalado ou nomeado)
4. Remova os seguintes arquivos do diretório /etc/rc3.d:
   - S98sentinel
   - S99wizard
   - S99esyslogserver (v5.1.1.1)
   - S99esdee (se o conector SDEE estiver instalado)
5. Remova os seguintes arquivos do diretório /etc/rc0.d:
   - K01wizard
   - K02sentinel
   - K01esdee (se o conector SDEE estiver instalado)
   - K01esyslogserver (v5.1.1.1)
6. Remova os seguintes arquivos do diretório /etc/init.d:
   - sentinel
   - assistente
   - esdee (se o conector SDEE estiver instalado)
   - esyslogserver (v5.1.1.1)

7. Remova os seguintes arquivos de /usr/local/bin:
   - restart_wizard.sh
   - stop_wizard.sh
   - start_wizard.sh
8. Referências do installshield de limpeza em /var/sadm/pkg. Remova os seguintes arquivos do diretório var/sadm/pkg:
   - Todos os arquivos que começam com IS (IS* na linha de comando)
   - Todos os arquivos que começam com ES (ES* na linha de comando)
   - Todos os arquivos que começam com MISCwp (MISCwp* na linha de comando)
9. Remova o usuário esecadm (e o diretório pessoal) e o grupo esec (verifique se ninguém fez login como usuário esecadm antes de realizar essa tarefa)
   - Execute: userdel -r esecadm
   - Execute: groupdel esec
10. Remova a seção do installshield de /etc/profile, /etc/.login
11. Remova o diretório /InstallShield, se houver um.
12. Remova o banco de dados do Sentinel Oracle seguindo as instruções na seção "Limpeza manual do banco de dados do Sentinel Oracle no Solaris"
13. Reinicie o sistema operacional.

Limpeza manual do banco de dados do Sentinel Oracle no Solaris

1. Como usuário do oracle, interrompa a escuta do Oracle:
   - Execute: lsnrctl stop
2. Pare o banco de dados do Sentinel:
   - Mude para o usuário do Oracle
   - Defina a variável de ambiente ORACLE_SID como o nome da instância do banco de dados do Sentinel (geralmente ESEC).
   - Execute: sqlplus '/ as sysdba'
   - No prompt sqlplus, execute: encerramento imediato
3. Remova a entrada para o banco de dados do Sentinel no arquivo /var/opt/oracle/oratab
4. Remova o arquivo init<your_instance_name>.ora (geralmente initESEC.ora) do diretório $ORACLE_HOME/dbs.
5. Remova as entradas para o banco de dados do Sentinel dos seguintes arquivos no diretório $ORACLE_HOME/network/admin.
   - tnsnames.ora
   - listener.ora
6. Apague os arquivos do banco de dados do local onde escolheu para instalá-los.

Linux

Limpeza manual do Sentinel no Linux

1. Efetue login como Usuário Root.
2. Verifique se todos os processos do Sentinel não estão sendo executados.
3. Remova os conteúdos de /opt/sentinelXX (ou onde o software do Sentinel foi instalado ou nomeado)
4. Remova os seguintes arquivos do diretório /etc/rc5.d:
   - S98sentinel
   - S99wizard
   - S99esyslogserver (v5.1.1.1)
   - S99esdee (se o conector SDEE estiver instalado)
5. Remova os seguintes arquivos do diretório /etc/rc3.d:
   - S98sentinel
   - S99wizard
   - S99esyslogserver (v5.1.1.1)
   - S99esdee (se o conector SDEE estiver instalado)
6. Remova os seguintes arquivos do diretório /etc/rc0.d:
   - K01esyslogserver (v5.1.1.1)
   - K01wizard
   - K02sentinel
   - K01esdee (se o conector SDEE estiver instalado)
7. Remova os seguintes arquivos do diretório /etc/init.d:
   - sentinel
   - assistente
   - esyslogserver (v5.1.1.1)
   - esdee (se o conector SDEE estiver instalado)
8. Remova os seguintes arquivos de /usr/local/bin:
   - restart_wizard.sh
   - stop_wizard.sh
   - start_wizard.sh
9. Remova o diretório /root/InstallShield
10. Remova o arquivo /root/vpd.properties
11. Remova o usuário esecadm (e o diretório pessoal) e o grupo esec (verifique se ninguém fez login como usuário esecadm antes de realizar essa tarefa)
    - Execute: userdel -r esecadm
    - Execute: groupdel esec
12. Remova a seção do installshield de /etc/profile, /etc/.login
13. Remova o banco de dados do Sentinel Oracle seguindo as instruções na seção " Limpeza manual do banco de dados do Sentinel Oracle no Linux".
14. Reinicie o sistema operacional.

Limpeza manual do banco de dados do Sentinel Oracle no Linux

1. Como usuário do oracle, interrompa a escuta do Oracle:
   - Execute: lsnrctl stop
2. Pare o banco de dados do Sentinel:
   - Mude para o usuário do Oracle
   - Defina a variável de ambiente ORACLE_SID como o nome da instância do banco de dados do Sentinel (geralmente ESEC).
   - Execute: sqlplus '/ as sysdba'
   - No prompt sqlplus, execute: encerramento imediato
3. Remova a entrada para o banco de dados do Sentinel no arquivo /etc/oratab
4. Remova o arquivo init<your_instance_name>.ora (geralmente initESEC.ora) do diretório $ORACLE_HOME/dbs.
5. Remova as entradas para o banco de dados do Sentinel dos seguintes arquivos no diretório $ORACLE_HOME/network/admin.
   - tnsnames.ora
   - listener.ora
6. Apague os arquivos do banco de dados do local onde escolheu para instalá-los.

Windows

Limpeza manual do Sentinel no Windows

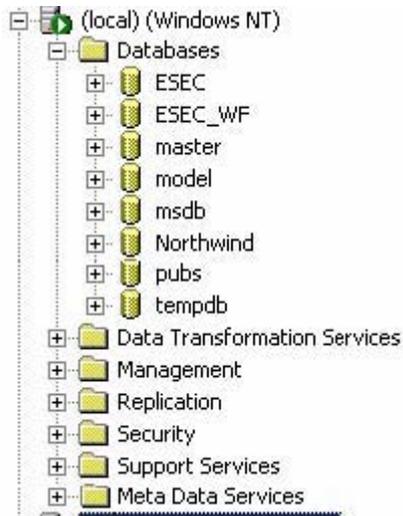
1. Apague a pasta C:\Program Files\Common Files\InstallShield\Universal e todo o seu conteúdo.
2. Apague a pasta de instalação antiga do Sentinel (e.g.- C:\Program Files\sentinel [%ESEC_HOME%]).
3. Apague as seguintes variáveis de ambiente (se houver) clicando com o botão direito em Meu Computador, selecionando Propriedades, clicando na guia Avançado, e no botão Variáveis de ambiente:
   - ESEC_HOME
   - ESEC_VERSION
   - ESEC_JAVA_HOME
   - ESEC_CONF_FILE
   - WORKBENCH_HOME
4. Remova todas as entradas no caminho variáveis de ambiente que levam a uma instalação anterior

   CUIDADO: Cuidado para remover somente caminhos para instalações antigas do Sentinel. Remover outras entradas no caminho pode resultar no funcionamento inadequado do sistema.

5. Apague todos os atalhos do Sentinel da sua área de trabalho.
6. Apague a pasta de atalhos *Iniciar* > *Programas* > *Sentinel* do menu Iniciar.

7. Remova o banco de dados do Sentinel Microsoft SQL Server seguindo as instruções na seção *Limpeza manual do banco de dados do Sentinel Microsoft SQL Server no Windows.*
8. Reinicie o sistema operacional.

Limpeza manual do banco de dados do Sentinel Microsoft SQL Server no Windows

1. Abra o Microsoft SQL Server Enterprise Manager e conecte a instância do SQL Server onde você instalou o banco de dados do Sentinel.
2. Expanda a árvore do Banco de Dados e localize o seu banco de dados do Sentinel.

3. Para cada um dos bancos de dados ESEC e ESEC_WF (ou qualquer nome que você deu ao banco de dados durante a instalação), clique com o botão direito no banco de dados e selecione *Apagar*.
4. Ao ser solicitado, selecione *Sim* para apagar o banco de dados.